NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

SHIPBOARD MICROCOMPUTERS AND THE
ADP ACCREDITATION PROCESS

by

Bruce Edward Nelson

September 1986

Thesis Advisor: Ken Euske

Approved for public release; distribution is unlimited

UNCLASSIFIED
CURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b RESTRICTIVE MARKINGS
SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION / AVAILABILITY OF REPORT Approved for public release; distribution is unlimited
DECLASSIFICATION / DOWNGRADING SCHEDULE	
PERFORMING ORGANIZATION REPORT NUMBER(S)	5 MONITORING ORGANIZATION REPORT NUMBER(S)
NAME OF PERFORMING ORGANIZATION aval Postgraduate School	6b OFFICE SYMBOL (If applicable) Code 54
7a NAME OF MONITORING ORGANIZATION Naval Postgraduate School	
ADDRESS (City, State, and ZIP Code) onterey, California 93943-5000	7b ADDRESS (City, State, and ZIP Code) Monterey, California 93943-5000
NAME OF FUNDING / SPONSORING ORGANIZATION	8b OFFICE SYMBOL (If applicable)
9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER	
ADDRESS (City, State, and ZIP Code)	10 SOURCE OF FUNDING NUMBERS

PROGRAM ELEMENT NO	PROJECT NO	TASK NO	WORK UNIT ACCESSION NO

TITLE (Include Security Classification)
HIPBOARD MICROCOMPUTERS AND THE ADP ACCREDITATION PROCESS

PERSONAL AUTHOR(S)
elson, Bruce E.

a TYPE OF REPORT	13b TIME COVERED	14 DATE OF REPORT (Year, Month, Day)	15 PAGE COUNT
laster's Thesis	FROM _____ TO _____	1986, September	124

SUPPLEMENTARY NOTATION

COSATI CODES		
FIELD	GROUP	SUB-GROUP

18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
Alternatives to formal risk analysis; The DON ADP Accreditation Process; An Evaluation of Accreditation Procedures for Shipboard Microcomputers

ABSTRACT (Continue on reverse if necessary and identify by block number)

The purpose of this thesis is to examine the Department of the Navy ADP system accreditation process as it relates to shipboard microcomputers. The primary reference document, OPNAVINST 5239.1A, is the Department of the Navy Automatic Data Processing Security Program instruction, which details the accreditation process. The accreditation process and limitations of the instruction are discussed.

An alternative method for determining ADP systems safeguards, the baseline security safeguard model used by the U.S. Geological Survey, is evaluated to determine its applicability in the shipboard microcomputer environment. Additionally, the Nelson/DOD model, which uses cost and proved effectiveness as metrics to select countermeasures, is developed and discussed.

0 DISTRIBUTION / AVAILABILITY OF ABSTRACT	21 ABSTRACT SECURITY CLASSIFICATION	
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	Unclassified	
2a NAME OF RESPONSIBLE INDIVIDUAL Prof. Ken J. Euske	22b TELEPHONE (Include Area Code) (408) 646-2860	22c OFFICE SYMBOL Code 54Ee

D FORM 1473, 84 MAR 83 APR edition may be used until exhausted
All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

#19 - ABSTRACT - (CONTINUED)

This thesis concludes that a more cost effective means of selecting countermeasures is needed and recommends that the Nelson/DOD model be adopted to accomplish this goal. Suggested further research involves creating a Decision Support System (DSS) by automating the Nelson/DOD model.

Approved for public release; distribution is unlimited.

Shipboard Microcomputers and the ADP Accreditation Process

by

Bruce Edward Nelson
Lieutenant, United States Navy
B.S., The University of South Carolina, 1977

MASTER OF SCIENCE IN INFORMATION SYSTEMS

from the

NAVAL POSTGRADUATE SCHOOL
September 1986

ABSTRACT

The purpose of this thesis is to examine the Department of the Navy ADP system accreditation process as it relates to shipboard microcomputers. The primary reference document, OPNAVINST 5239.1A, is the Department of the Navy Automatic Data Processing Security Program instruction, which details the accreditation process. The accreditation process and limitations of the instruction are discussed.

An alternative method for determining ADP systems safeguards, the baseline security safeguard model used by the U.S. Geological Survey, is evaluated to determine its applicability in the shipboard microcomputer environment. Additionally, the Nelson/DOD model, which uses cost and proved effectiveness as metrics to select countermeasures, is developed and discussed.

This thesis concludes that a more cost effective means of selecting countermeasures is needed and recommends that the Nelson/DOD model be adopted to accomplish this goal. Suggested further research involves creating a Decision Support System (DSS) by automating the Nelson/DOD model.

TABLE OF CONTENTS

I. INTRODUCTION

A. SUMMARY

The purpose of this thesis is to examine the Department of the Navy (DON) accreditation process, in general, and how it specifically relates to the shipboard microcomputer environment. The goal of the DON Automated Data Processing (ADP) security program is accreditation of all DON ADP systems and networks, based on a review of the existing ADP security posture. The purpose of accreditation is to ensure the activity or network is operating at an acceptable level of risk. Within the DON, accreditation is defined as a policy decision by the responsible Designated Approving Authority (DAA). Accreditation results in a formal declaration that appropriate security countermeasures have been properly implemented for the ADP activity or network.

OPNAVINST 5239.1A is the Department of the Navy Automated Data Processing Security Program instruction. The most significant limitation of OPNAVINST 5239.1A is that it lacks a valid method for making cost effectiveness a selection criterion for countermeasures. The metric used for selecting countermeasures is return on investment (ROI), the ratio of annual savings to annual cost of additional countermeasures. The annual savings is comprised of the difference between the estimated annual loss expectancy

(ALE) of the ADP system before and after countermeasures are installed. The method is questionable because it uses estimates which are difficult to predict accurately. A method is needed which provides a systemic approach to determining an ADP system's most cost effective countermeasures.

It can be argued that another limitation of OPNAVINST 5239.1A is that it is oriented toward main frame operations and assumes a high level of organizational computer expertise. This assumption may not hold true for organizations using mini or microcomputers. Further, this assumption complicates the accreditation process because such organizations often lack individuals skilled in formal ADP administrative procedures. Consequently, simplified alternative approaches to the accreditation process should be examined and developed.

B. AN ALTERNATIVE

Cecula (1985) advocates the use of baseline security safeguards in organizations with many similar ADP facilities. He postulates that if multiple risk analyses were conducted patterns would become apparent and the resulting recommendations would be similar. A central assumption of this thesis is that ADP (microcomputer) installations in the surface fleet fit this description. If a risk analysis were conducted for every ship in the fleet implementing a microcomputer system, patterns would become

apparent and the resulting recommendations would be very similar, indicating that the baseline approach for security safeguards may be appropriate. An example of an emerging pattern would be that the microcomputer systems aboard different ships are being used for a common purpose by the same groups of individuals (e.g., the COs, XOs, and Department Heads of these ships), processing similar information, and using similar hardware and applications programs.

For instance, the senior watch officers are all responsible for maintaining the viability of their respective in-port and at sea watch organizations. They can use a microcomputer data base application to track watchstanders, their qualifications, and rotation dates. The operations officers are all responsible for maintaining their ships' Unitreps (Unit Reporting System). They can also use a data base program to track selected exercises, personnel information, information pertinent to the ship's schedule, and the status of outstanding material casualties. The legal officers are responsible for generating the necessary documents for administrative discharge proceedings. They may be inputting this information into standardized formats using a word processing program. The use of standard operating procedures and the author's past professional experience indicates that there are no

significant differences in who uses these systems, how the systems are used, or what the systems uses are.

C. METHODOLOGY AND ASSUMPTIONS

This thesis provides a general, standardized model which satisfies the initial accreditation requirements as set forth in OPNAVINST 5239.1A. The method is developed by first discussing and analyzing the DON accreditation process. Limitations of the DON model are then addressed and alternatives examined.

The model developed in this thesis is based upon a generalization of this shipboard ADP environment and makes the following assumptions:

- the level of data processed is Level I, classified information; Level II, unclassified information requiring special protection; and Level III, all other unclassified data.

- the security mode of operation is the Dedicated Security Mode. An ADP system is operating in the dedicated security mode when the Central Computer Facility and all of its connected peripheral devices and remote terminals are exclusively used and controlled by specific users or group of users having a security clearance and need-to-know for the processing of a particular category(ies) and type(s) of classified material.

- the ADP system configuration and locations consist of stand alone microcomputers located in spaces with controlled access.

- the criticality of the mission is low, the present manual system can be used effectively, although somewhat less efficiently.

The following outline provides an overview of this thesis:

CHAPTER 1. The first chapter provides a discussion of the DON accreditation process.

CHAPTER 2. The second chapter is an evaluation of the first step in the accreditation process: risk analysis.

CHAPTER 3. The third chapter is a summary of the remaining steps in the accreditation process.

CHAPTER 4. The fourth chapter is an evaluation of the USGS baseline security model.

CHAPTER 5. The fifth chapter is a proposed alternative to conducting a risk analysis.

CHAPTER 6. The sixth chapter is a summary of conclusions and recommendations.

II. THE ACCREDITATION PROCESS

This chapter provides a discussion of the key elements of the accreditation process. Guidance pertinent to achieving ADP system accreditation is found in OPNAVINST 5239.1A, the Department of the Navy Automated Data Processing Security Program.

A. GENERAL

The Designated Approving Authority (DAA) is an official assigned responsibility to accredit ADP elements, activities, and networks under that official's jurisdiction. Specific identification of this individual depends upon the ADP environment; defined by the level of data processed, the security mode of operation, ADP system configurations and locations, and the criticality of the ADP system to the organization's mission.

Accreditation is the DAA's formal declaration that appropriate ADP security countermeasures have been properly implemented for the activity's ADP systems or networks consistent with the particular level of data protection required and that the applicable steps in the accreditation process identified by the DAA are complete.

The accreditation process is the means whereby information pertaining to the security of an activity's ADP computer systems or networks is collected, analyzed, and

submitted for approval to the appropriate DAA. The individual steps of the accreditation process vary by level and type of data. Accreditation requirements are defined by Department of Defense, Director of Central Intelligence, and Department of the Navy regulations. The DAA is responsible for ensuring that the pertinent instructions and regulations are followed. The DAA evaluates his activity's ADP program to ensure compliance.

Naval activities are either accredited or not accredited. If an activity is not accredited, computer systems or networks may operate if the appropriate DAA has issued an interim authority to operate. Interim authority to operate is:

- granted for a fixed period, generally one year,
- based upon an approved activity ADP security plan,
- contingent upon certain conditions being met (e.g., standard operating procedures being strengthened or TEMPEST[1] being certified).

Accreditation becomes effective when a formal, dated statement of accreditation is issued. The statement of accreditation will identify:

- the computer systems or networks being accredited,
- the applicable level of data,
- the security mode of operation.

---

[1]TEMPEST is defined as the study and control of spurious electronic signals emitted from ADP equipment.

A review will then be made at least every five years to verify that accreditation is still merited. This action may occur sooner if the DAA determines that a change has been made which voids the accreditation conditions.

B. ACCREDITATION REQUIREMENTS FOR LEVEL I AND LEVEL II DATA

As discussed in the introduction, shipboard microcomputer systems have the capability to process classified data (Level I) or unclassified data requiring special protection (Level II) and do so in the dedicated mode, which according to OPNAVINST 5239.1A makes the commanding officer the DAA. Commanding officers who are their own DAA will:

(1) Conduct a risk assessment,

(2) Develop a Security Test & Evaluation Plan (ST&E) and conduct an ST&E,

(3) Document the ST&E test results,

(4) Develop a Contingency Plan,

(5) Develop an Activity ADP Security Plan (AADPSP) and submit it for COMNAVDAC approval,

(6) Prepare the accreditation support documentation,

(7) Issue a Statement of Accreditation as described in paragraph 3.3c of OPNAVINST 5239.1A,

(8) Forward information copies of the Statement of Accreditation to COMNAVDAC.

This thesis is concerned mainly with the accreditation process as it relates to the shipboard microcomputer environment where the Commanding Officer is the DAA.

The next chapter discusses risk analysis, the first step in the process. Steps 2-8 are addressed in Chapter 3.

III. RISK ANALYSIS

A. GENERAL

The initial step in the accreditation process is to conduct a risk analysis. Two methods are used by the DON for conducting risk analyses, which are outlined in Appendix E of OPNAVINST 5239.1A. Appendix E recommends that an ADP Security Survey be conducted first in order to determine which of the two methods should be used by defining the scope of the risk analysis effort. The purpose of this chapter is to present the ADP security survey and risk analysis for the use of microcomputers aboard cruiser/destroyer type ships. The risk analysis is accomplished using the method indicated by the security survey.

Within this chapter the ADP security survey and risk analysis Methods I and II are briefly discussed. Then the ADP security survey and risk analysis method used in the shipboard microcomputer environment are evaluated. Finally, an ADP Security Survey pertinent to shipboard microcomputers is included as Appendix A of this thesis.

B. OPNAVINST 5239.1A ADP SECURITY SURVEY

The ADP Security Survey has two sections. The first section describes the ADP system and the second section

summarizes the site security profile, which encompasses environmental issues and physical security.

The information contained in the survey is derived from the author's knowledge of the shipboard environment and the knowledge of ADP security specialists from NARDAC San Francisco, California. The information is accurate to the extent that it is representative of what one would expect to find, in most ships, consistent with established policies and practices. Limitations of the structure of the ADP survey are addressed later in this chapter.

C. OPNAVINST 5239.1A RISK ASSESSMENT METHODOLOGY

A risk assessment involves a detailed examination of the assets and procedures of the ADP activity. An enumeration of the ADP activity's vulnerabilities and the threats that may exploit the vulnerabilities, resulting in destruction, disclosure, or modification of data, or denial of ADP services is critical to the successful completion of the risk analysis. Additionally, a risk assessment considers the current status and mission of the ADP activity. The DAA (as stated above, in the case of a ship the DAA is the commanding officer) determines which risk assessment methods will be used based on the complexity of the ADP environment, as determined in the ADP Security Survey (see Appendix A). As previously stated the ADP environment is governed by the level of data processed, the security mode of operation, the

ADP system configurations and locations, and the criticality of the ADP system to the organization's mission.

Two risk assessment methods are provided in Appendix E of OPNAVINST 5239.1A. Method I is the standard method for use in most ADP environments. Method II is for use in less complex ADP environments.

D. METHOD I OVERVIEW

Risk Assessment Methodology I as presented in OPNAVINST 5239.1A consists of the following major steps.

1. Asset Identification and Valuation

a. List and describe each asset. Particular attention should be given to valuation of data assets since these typically represent the greatest risk of substantial loss.

b. For each asset determine the impact value for each applicable impact area, where impact is defined as destruction, disclosure, modification of data, or denial of service to users. (Impact value ratings are found in OPNAVINST 5239.1A, Table E-2.)

c. Provide documentation to support the impact value rating assigned and identify the cost included in the impact values.

2. Threat and Vulnerability Evaluation

a. List and describe all the threats, vulnerabilities, and existing countermeasures against each threat.

b. Give examples of how the threats might exploit the vulnerabilities and penetrate the existing countermeasures.

c. Indicate the impact area(s) to which each threat applies.

d. Estimate the frequency of successful attack for each applicable impact area for the threat.

e. Justify the selected frequency of successful attack.

3. Computation of the Annual Loss Expectancy (ALE)

Calculate the estimated potential annual dollar loss to the activity based upon the identified threats, vulnerabilities, and existing countermeasures, thus determining the activity's overall ADP security posture. This calculation is called the ALE and represents a quantitative estimate of the potential average yearly financial loss resulting from modification, destruction, or disclosure of data, or denial of services because of existing vulnerabilities (i.e., flaws or weaknesses) which may permit identified threats to be realized. The ALE provides a dollar value baseline for determining the current ADP security posture and for accomplishing a cost-benefit analysis of new countermeasures under consideration.

4. Evaluation and Selection of Additional Countermeasures

a. Identify additional countermeasures which could be applied to the activity.

b. Evaluate the effectiveness of each proposed countermeasure to reduce the identified vulnerability and indicate the impact on the frequency of successful attack for the applicable threat(s).

c. Determine the cost-effectiveness of each proposed countermeasure by analyzing the effect of its implementation on the ALE caused by the reduction in the frequency of successful attack. For a countermeasure to result in a monetary savings, the amount saved over the life cycle of the countermeasure must exceed the cost of installation and implementation. Any countermeasure which satisfies this test is cost-effective. Threats which have the greatest potential

for harm based on their impact on the ALE indicate where to apply countermeasures.

d. Recommend to the commanding officer an implementation schedule for all countermeasures having a return on investment (ROI) greater than one.

5. Proceed with Accreditation Process

A brief comment regarding Step 2 is in order before proceeding. If Level I or II data are processed by the system, then this portion of the risk assessment should be classified at a level appropriate to that data, failure to do so could result in exceptionally grave consequences. This has not been directed by OPNAVINST 5239.1A, however, it seems appropriate.

E. METHOD II OVERVIEW

Risk Assessment Methodology II contains all of the essential elements of Method I, but does not provide the degree of detail of Method I. Also Method II does not provide for the interaction of threats and evaluation of threats by impact areas as does Method I. It is therefore limited to use in less complex ADP environments.

Risk Assessment Methodology II as presented in OPNAVINST 5239.1A consists of the following major steps.

1. Asset Identification and Valuation

All of the assets of the ADP activity or network are identified and assigned a dollar value based on the impact of modification, destruction, disclosure, and denial of

service. In all cases, the risk assessment documentation will provide justification for the dollar values assigned.

2. Threat and Vulnerability Evaluation and Annual Loss Expectancy (ALE) Computation

All of the threats are identified and assigned a threat value based on the probability that they will exploit vulnerabilities and successfully attack an asset. The threat values are based on available information and experience, evaluating vulnerability in the light of existing countermeasures.

The document used to compute the ALE is the risk assessment matrix. Assets and their impact values are listed in columns and the threats are listed in rows. The ALE computation step is a series of mathematical computations which reflects the summation of the products of all impact values (the value of loss or compromise of the asset) and threat values (the probability that the threat will occur). (This process assumes threats are mutually exclusive and does not account for their interaction.)

3. Selection of Additional Countermeasures

The total ALE provides a measure of the current command security practices, the risks, and provides a baseline for evaluating which additional countermeasures would best improve the overall ADP security posture. Countermeasures intended to significantly reduce the vulnerabilities posed by the threats having the highest annual loss expectancies are to be implemented first.

The document used to determine priorities of the additional countermeasures is the additional countermeasures selection worksheet. A revised ALE is calculated using the reduced threat value in light of the additional countermeasure to be implemented. The annual savings is the difference between the original and revised ALE's. The return on investment is calculated by dividing the annual savings by the annual cost of the countermeasure. Countermeasures are normally implemented in descending order based upon return on investment. Deviations from this guideline may be necessary because of budget constraints and requirements of higher authority.

F. SUMMARY

Detailed procedures, forms, and tables for completing the risk assessment are provided in Appendix E of OPNAVINST 5239.1A. Assets should be categorized as: (1) software, (2) data, (3) hardware, (4) administrative, (5) physical, (6) personnel, or (7) communication. The dollar amount assigned to an asset for each impact area (destruction, disclosure, and modification of data, denial of service to users) represents the importance of not allowing the particular type of damage to occur. In other words, the dollar amount assigned represents how much money should reasonably be spent to avoid a single incident of the type being considered.

In all cases the risk assessment documentation must:

- document the assumptions used in determining asset dollar values,
- provide documentation to support the impact value rating assigned and identify the costs included in the impact value.

G. ANALYSIS OF THE ADP SECURITY SURVEY

One limitation of the OPNAVINST 5239.1A Security Survey, contained in Appendix E of the instruction, is that it does not provide the DAA with a valid means of determining whether to use Risk Assessment Method I or Method II, the stated purpose for conducting the survey. There is no quantitative measure or logical design which gives clear-cut guidance regarding which method should be used.

Section I, question B asks for the dollar value impact of loss and cost to replace. At least two problems occur which highlight the difficulty of providing clear-cut quantitative guidance:

- First, the dollar value for data ultimately used in the Annual Loss Expectancy calculation, appears to be more oriented toward justifying expenditures for countermeasures than reflecting the true impact of compromise. (For instance, step 3 of Risk Assessment Method I states that the ALE provides a dollar value baseline for determining the current ADP security posture and for accomplishing a cost-benefit analysis of new countermeasures under consideration). Additionally, the impact of the loss of classified information in dollar terms and the probability that a threat impacts an asset may be impossible to accurately assess.
- Second, the amounts disregard the anticipated life of the equipment. The values should be discounted to provide a net present value analysis, which would provide a more accurate assessment of system value versus present cost.

Section II of the survey lists several vulnerabilities and the operating countermeasures and asks the respondent to assess the risk as high, moderate, or low. Appendix F of OPNAVINST 5239.1A provides limited guidance relative to how this is to be accomplished. For instance, section F.2 provides some guidance for completing the security survey as it relates to software countermeasures. However, the terms high, medium, and low used to describe the confidence level associated with these countermeasures are only defined in general terms (e.g., the confidence level for password protection from visual observation: "Suppressing the printing of the password is rated high, while other protection mechanisms are rated medium"). The respondent must make a subjective evaluation of the countermeasures' effectiveness. Also, section F.3 provides some guidance for completing the security survey as related to hardware countermeasures. Again the respondent must subjectively evaluate the countermeasures' effectiveness. An example is the level of confidence provided by Protection-State Variables, "Depending upon how well the system software uses protection-state variables, this countermeasure ranges from low to high."

As the analysis suggests, the choice of whether to use Method I or II is based primarily upon subjective judgments of the DAA.

H. AN ALTERNATIVE TO THE ADP SECURITY SURVEY

A pragmatic approach that is most often used in practice by security specialists at NARDAC, San Francisco, California, is to determine which method to use based on the following three criteria:

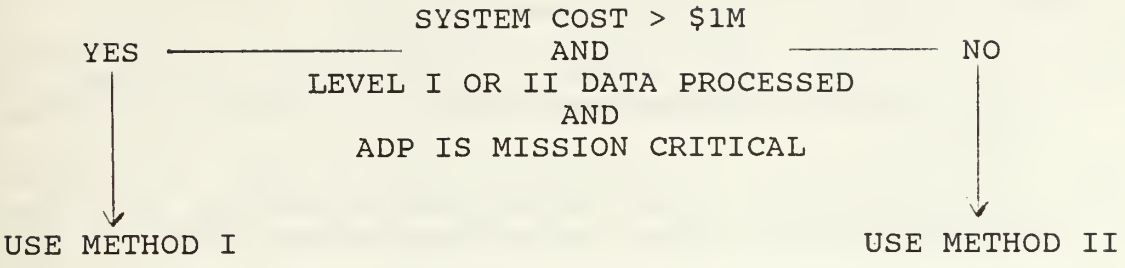
- if the system cost exceeds some minimum amount (in practice approximately $1,000,000),
- and Level I or II data are used in the system (classified information and unclassified information requiring special protection),
- and the ADP system is critical to the accomplishment of the organization's mission;

then Risk Assessment Method I is used. If any one of the three criteria is not met, then Method II is used. This approach is used because the survey does not provide the DAA with adequate guidance (Sharp, 1986).

The first two criteria can be evaluated on the basis of archival data. Evaluation of the third criterion is made as follows: If nothing else changes, could the activity accomplish its mission without the use of the ADP system? This is a question which the DAA should be able to answer without much difficulty.

The following decision matrix depicts the decision graphically.

Using the pragmatic approach, Risk Assessment Method II should be used in the shipboard microcomputer environment. This is true because the first and third criteria are not



met, the system cost is less than $1,000,000 and the shipboard microcomputer system is not mission critical.

Appendix B contains a completed Risk Assessment for the use of shipboard microcomputers using Method II. The risk assessment matrix and additional countermeasures worksheet were completed in accordance with instructions outlined in Appendix E of OPNAVINST 5239.1A and Chapter II of this thesis. The risk assessment matrix is a summary of the threats associated with the shipboard microcomputer environment. The additional countermeasures selection worksheet lists respective countermeasures which will reduce the threat. Threat values were taken from Table E-1 of OPNAVINGST5239.1A. Prices for the countermeasures were taken from a recent computer products catalogue (DEVOKE Data Products, Summer/Fall 1985).

The following section is an analysis of the risk assessment process which discusses some of the limitations associated with Method II.

I. ANALYSIS OF RISK ASSESSMENT METHOD II

There are at least three problems with the method used for conducting microcomputer risk analysis:

(1) One is that even though this method is for use in less complex ADP environments, it is still mainframe oriented.

(2) The second involves the method currently used for calculating the Annual Loss Expectancy (ALE).

(3) The third arises from the practice of selecting countermeasures based upon their respective ROI.

The first problem is understandable in that the Navy has amassed far more experience in the mainframe environment than any other. However, this places an undue burden on activities which must use Method II, but do not have the level of computer expertise that would be found in the mainframe environment. In the short term this creates a problem. In the long term, as the use of microcomputers proliferates, instructions will become oriented toward a more diverse audience and at the same time the individuals using the instructions will be more "computer literate." (Nolan, 1975)

The second problem requires a different type of analysis. The ALE has two components, the impact value rating (the dollar impact of disclosing sensitive data) and the threat values (the probability that the threat will occur). The ALE is the product of the impact value rating and the threat value, summed for each asset to yield the TOTAL ALE BY INDIVIDUAL THREAT. The ALE's for each

individual threat are then summed to determine the TOTAL ALE. However, the dollar value of compromised classified information is difficult to determine. Therefore, impact values, based on the estimated damage caused by compromised classified information, are suspect. Additionally, even if the methods used to calculate threat values were sound, the threat values must be rated as either high, medium, or low, but no quantitative guidance regarding what constitutes a high, medium, or low probability is given. Personnel conducting the risk assessment are therefore left with their best judgment and the use of historical data, if available, to determine the range of values which defines whether the threat for a given asset is high, medium, or low. The validity of the process is further diluted when the system type is new and little historical data exists to support quantitative analysis.

One interpretation of the method used to calculate the ALE is that if one manipulates the numbers and argues persuasively enough (which the method allows) the cost of any countermeasure can be justified. This could foster an atmosphere of free spending which clearly violates the tenets of the DON acquisition process. The author's opinion is that a more cost effective means for identifying and fulfilling ADP security requirements can be developed.

The third problem is that selecting countermeasures based upon ROI does not support a systemic approach to

providing ADP system security. For instance, if two or more countermeasures, operating interactively, provide the optimum ADP system security, it is unlikely that Method II (or Method I) will reveal this (i.e., that the respective countermeasure's ROI will indicate the optimal system configuration).

A strong argument can be made that in the shipboard microcomputer environment, providing security while processing Level I information in the dedicated security mode is people dependent. The dominant consideration is that access to information is granted based o the individual processing the information possessing the appropriate security clearance and the need to know. The shipboard microcomputer system, by itself, does not impose any unique security requirements (with the exception of TEMPEST considerations).

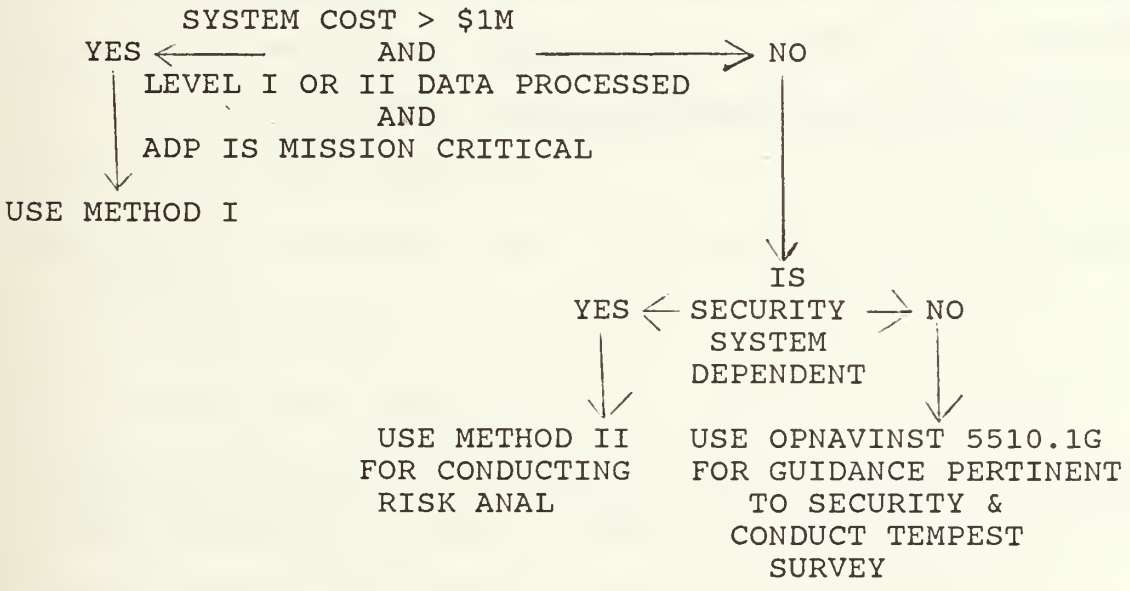
J. PERSONNEL AND INFORMATION SECURITY

OPNAVINST 5510.1G is the Navy's Personnel and Information Security Manual. This instruction contains provisions for the assignment of an ADP Security Officer and provides guidance pertinent to the administration of personnel and information security.

Personnel and information security depends heavily upon procedural controls. The officers and men serving onboard ships are familiar with personnel and information security procedures and the shipboard environment provides the

required administrative support (e.g., security clearances are maintained and access to classified information is granted on a need-to-know basis). Given the argument that the shipboard microcomputer system, in and of itself, does not impose any unique security requirements and OPNAVINST 5510.1G contains provisions for the assignment of an ADP Security Officer and provides guidance pertinent to the administration of personnel and information security, one approach would be to cover microcomputers under this instruction.

If this were done, the following decision diagram would depict the decision process discussed above:



William E. Perry, the executive director of the Quality Assurance Institute, Orlando, Florida, supports this analysis of the microcomputer security problem. Perry

(Perry, 1986) cites the following questions which must be addressed relative to microcomputer security:

- "Didn't end users already have the same information before the advent of microcomputers?"
- "Do microcomputers really pose a significantly new security risk?"
- "Aren't the existing security policies, procedures, and standards adequate to address microcomputers?"

His analysis concludes that the problem is personal security not microcomputer security. The information and programs of security concern are given to individuals, not machines. Therefore, the real problem is a people security problem and not a computer problem. If security is directed at machines, it misses the real problem. He further states that hardware and diskette security is a physical security problem. The key is to establish and follow policies and procedures laid down by management.

IV. STEPS IN THE ACCREDITATION PROCESS, THE REST OF THE STORY

The preceding chapter dealt with the first and most controversial step in the accreditation process: risk assessment. This chapter provides a discussion of the remaining steps in the accreditation process. While the discussion is general, the focus is on the process as defined by the shipboard microcomputer environment in which the commanding officer is the DAA. Table 4.1 lists the steps in the DON Accreditation Process as set forth in OPNAVINST 5239.1A.

TABLE 4.1

DON ACCREDITATION PROCEDURES, OPNAVINST 5239.1A

(1) Conduct a risk assessment

(2) Develop a Security Test & Evaluation Plan and conduct (ST&E)

(3) Document the ST&E test results

(4) Develop a Contingency Plan

(5) Develop an Activity Automated Data Processing Security Plan (AADPSP) and submit it for Commanding Officer Naval Data Automation Command (COMNAVDAC) approval)

(6) Prepare the accreditation support documentation

(7) Issue a Statement of Accreditation as described in paragraph 3.3c

(8) Forward information copies of the Statement of Accreditation to COMNAVDAC

A. STEP 2: DEVELOP A SECURITY TEST & EVALUATION AND CONDUCT A SECURITY TEST & EVALUATION

When the commanding officer is the DAA, the ST&E is the activity's responsibility. The scope of the ST&E depends on the level of data processed and the security mode of operation. The results of the risk assessment determine the level of detail and scope required for the ST&E.

The purpose of conducting an ST&E is to obtain technical information to help the DAA decide whether or not to accredit an ADP activity or network. The ST&E consists of two interrelated phases. The first phase determines whether the necessary countermeasures have been installed, and the second phase determines whether the installed countermeasures are working effectively.

1. Mandatory Procedures

The following steps are applicable to all ADP activities for which the commanding officer is the DAA.

a. Identify qualified individuals to perform the steps outlined below:

(1) ADP security

(2) System software/hardware

(3) Application software

(4) Telecommunications

(5) Emanation security

(6) Physical security

(7) Personnel, procedural, and administrative security

(8) User/customer functions: OPNAVINST 5239.1A states that when possible, it is preferable for each step to be performed by different individuals. Because of the scope of the microcomputer system used in the shipboard environment (cruisers/destroyers) this will neither be possible nor necessary. It would be coincidental that qualified ADP personnel are assigned in combatants because these ships do not require personnel with ADP skills. It is therefore unlikely that there will be enough qualified ADP personnel so that a different person can perform each of the steps. Additionally, in the shipboard microcomputer environment, given the necessary reference material, one person should be able to complete all 8 steps easily.

b. Review the risk assessment for currency and accuracy. Identify and analyze the nature of the threats and vulnerabilities and their respective countermeasures. This provides the basis for the development of the ST&E plan.

c. Develop the ST&E plan. The plan should describe how each countermeasure is to be tested in order to determine its effectiveness. If unanticipated situations arise while the ST&E is being conducted, the ST&E should be modified accordingly.

(1) The ST&E should address all elements of the ADP security environment:

- Hardware
- Software
- Physical facility/security
- Personnel
- Communications
- Emanations
- Administrative/operating procedures
- Data

(2) The ST&E plan should include the following items for each element in (1) above:

- Test objectives
- A Plan of Action & Milestones (POA&M) for the test
- The test team organization
- Detailed test plans and procedures
- Test data
- Execute the ST&E plan
- Document the results of the ST&E.

B. STEP 3: DOCUMENT THE ST&E TEST RESULTS

The ST&E report documents the execution and results of the ST&E plan. The ST&E report also analyzes the findings of the ST&E plan and lists recommendations to correct deficiencies. The following is a sample ST&E report format taken from Appendix H of OPNAVINST 5239.1A.

Index

Executive Summary

Body of Report:

1. ADP Security Environment
   a. Hardware Configuration
   b. Software
   c. Physical Facility/Security
   d. Personnel
   e. Communications
   f. Emanations

g. Administrative/Operating Procedures

h. Data

2. Test Objectives

3. Test Results and Analysis

a. Test results for each area and scenarios used

b. Overview of general findings and recommendations

c. Specific findings for each area

- Summary of problem
- Analysis of problem
- Alternative solutions
- Recommended solutions
- Cost to implement, either actual or projected, in terms of dollars or work hours
- impact on system operation

4. Analysis and recommendations regarding test approach and procedures and future system security testing.

5. Proposed POA&M for corrective actions and assignment of responsibilities.

C. STEP 4: DEVELOP A CONTINGENCY PLAN

The Contingency Plan should fully document procedures for continuity of operations. The detail and scope of the plan depends upon the characteristics of the individual activity. The activity contingency plan should provide detailed procedures for all aspects of emergency, backup, and recovery operations.

D. STEP 5: DEVELOP AN ACTIVITY AUTOMATED DATA PROCESSING SECURITY PLAN (AADPSP) AND SUBMIT IT FOR COMMANDING OFFICER NAVAL DATA AUTOMATION COMMAND (COMNAVDAC) APPROVAL

The activity ADP Security Plan (AADPSP) is a document which establishes and updates an activity's ADP security program. The purpose of the AADPSP is to:

- promulgate activity ADP security policy and provide guidelines for all ADP security procedures to be used by the activity,
- document the current ADP security environment, establish program objectives, and outline a POA&M for program implementation. The POA&M is critical to the success of the AADPSP. It identifies all activity ADP elements and outlines a schedule for completing the steps of the accreditation process for each ADP element.

Appendix H of OPNAVINST 5239.1A discusses the AADPSP and indicates that it should address the following areas:

1. The scope of the AADPSP.
2. The commanding officer's policy statement.
3. The ADP security organization and assignment of responsibilities.
4. Objectives for implementing the DON ADP security program at the activity.
5. An overview of the current ADP security environment to include:
   (a) Hardware
   (b) Software
   (c) Physical facility/security
   (d) Personnel
   (e) Communications
   (f) Emanations

(g) Administrative/operating procedures

(h) Data

6. Training

7. Audit/internal review

8. Provisions for ADP security in life cycle management

9. Provisions for ADP security in hardware and software configuration control

10. Activity accreditation schedule identifying all ADP elements and a POA&M for completing:

(a) Risk assessments

(b) ST&Es

(c) Contingency planning and testing

(d) Accreditations

The AADPSP serves as a comprehensive document detailing the commanding officer's desired security posture and the ADPSO's plans for achieving these objectives. It should be a living document for developing, updating, improving, maintaining, and managing ADP security requirements within the DON ADP activity. The ADPSO is responsible for developing, implementing, and updating the AADPSP.

E. STEP 6: PREPARE THE ACCREDITATION SUPPORT DOCUMENTATION

The purpose of the Accreditation Support Documentation is to provide information to support the request for accreditation. It provides evidence that the ADP activity has effectively implemented appropriate countermeasures consistent with the protection requirements for the data level and security mode of operation to be authorized.

Appendix H of OPNAVINST 5239.1A, section H.2.8 provides guidance for preparing the accreditation support documentation.

The documentation includes information requested by the DAA, such as:

1. the name, position, and telephone number of the ADP Security Officer (ADPSO) and ADP System Security Officer (ADPSSO) who will serve as a primary point of contact for the accreditation;

2. the identification and location of all Automated Data Processing Equipment (ADPE), also equipment layout charts and engineering diagrams;

3. line diagrams showing interconnection of ADPE, communications lines, and protection of the lines;

4. the approximate percentage of each application category of data to be processed (identified by project or task) versus the level of data (Level I, II, or III) and the type within each level (e.g., classified, personal, financial);

5. a description of the operating system and application software for ADP system, also descriptions of communications and network dependent applications software for networks, if applicable;

6. the current and proposed security modes of operation;

7. a copy of the ADP Security Operating Procedures and other applicable command security directives (e.g., security incident handling procedures, procedures for control of operating system and application software modification);

8. the risk assessment documentation;

9. descriptions of all countermeasures;

10. copies of previous system/network accreditations and interim authorities to operate;

11. certification of compliance with security directives;

12. the ST&E test plans;

13. the ST&E test reports;

14. TEMPEST accreditation, if applicable;

15. physical accreditation, if applicable;

16. the Contingency Plan;

17. the Contingency Plan test results;

18. the AADPSP;

19. and other documentation as required by ADPSO.

F. STEP 7: ISSUE A STATEMENT OF ACCREDITATION

A sample statement of accreditation is contained in Appendix H of OPNAVINST 5239.1A, Figure H-7.

G. STEP 8: FORWARD INFORMATION COPIES OF THE STATEMENT OF ACCREDITATION TO COMNAVDAC

H. ANALYSIS AND COMMENTS ON STEPS 2 THROUGH 8

Steps 2 through 8 provide the follow-up and validation for the result of Step 1, the risk analysis.

1. Steps 2 and 3

Both are concerned with developing the ST&E, conducting the test, and documenting the results. The test has two interrelated phases:

- determine whether or not the necessary countermeasures have been installed,
- determine whether the installed countermeasures are working effectively.

The first phase must ask the same question that is asked in the risk analysis. As is the case with risk analyses, determining whether or not the necessary

countermeasures have been installed requires that the threat be identified and well defined. The second phase is an evaluation of the how effective the installed countermeasures are. Since this model selects the countermeasure with the highest ROI as determined by the risk analysis (which has already been identified as an imprecise, subjective process), two questions arise:

- is the countermeasure selected technically sufficient to counter the threat, and
- is the countermeasure selected the most cost effective to counter the threat.

Step 2 is designed to answer the first question. Unfortunately, due to the limitations associated with risk assessments, this model is unable to adequately answer the second question, a severe limitation. Periods of national fiscal austerity evinced by legislation such as Gramm, Rudman, Hollings initiatives dictates that we make cost effectiveness a priority.

Appendix C contains an abbreviated ST&E used in conjunction with risk assessment Method II. This document was developed by the Naval Electronic Systems Engineering Activity, St. Inigoes, Maryland, and provides useful guidance.

2. Step 4

Because the shipboard microcomputer system is not mission critical, a contingency plan is not required. A loss of processing capability for a reasonable period of

time would be inconvenient, but would not adversely affect the ship's mission since its function is administrative. If alternate hardware exists, however, its location shall be specified as well as the location of data/software diskettes, back-up diskettes, and supplies, in accordance with good management practice. Appendix D is a sample Contingency Data Form used by NARDAC, San Francisco, which is suitable for use in the shipboard microcomputer environment.

3. Steps 5 Through 8

The AADPSP is basically a policy statement which includes guidelines and a timetable for meeting program objectives. Steps 6 through 8 are procedural.

Theoretically, with minor modifications to how countermeasures are selected, Steps 2 through 8 could be used independent of the risk analysis process if an acceptable alternative for conducting risk assessments were identified. The ability of a particular methodology to ensure cost effectiveness is the criteria which establishes acceptable alternatives.

V. THE US GEOLOGICAL SURVEY BASELINE SECURITY MODEL

A. INTRODUCTION

The baseline security model was developed by the USGS because models which had been used previously were directed toward large computer centers. The premise was that these models were inappropriate for use in their microcomputer installations, which were expanding in number. Factors critical to development of the baseline security model were the organizational structure and the computer security environment within the USGS.

B. GENERAL

The method employed within the USGS baseline security model:

- determines which of six categories describes the computer system in question, and
- implements the minimum acceptable security requirements for that category.

The three system attributes which must be reviewed in order to determine the computer system category are:

- data sensitivity,
- the system's users, and
- access afforded the system & data resources (Cecula, 1985).

Figure 5.1 is a tree diagram which represents how the USGS security category is determined. The first

determination is whether or not the data are sensitive. Data are sensitive if they are proprietary, critical to the mission of one of the agencies programs, or personal information. The second determination concerns the computer systems' users or user groups. If there is only one user or a small group of users with homogenous needs, then the system is characterized as a single user system. The third determination involves physical access to the computer system. If system users can only gain access through another party then access is controlled. The set of minimum security requirements is then defined by the category of the computer system (Cecula, 1985).

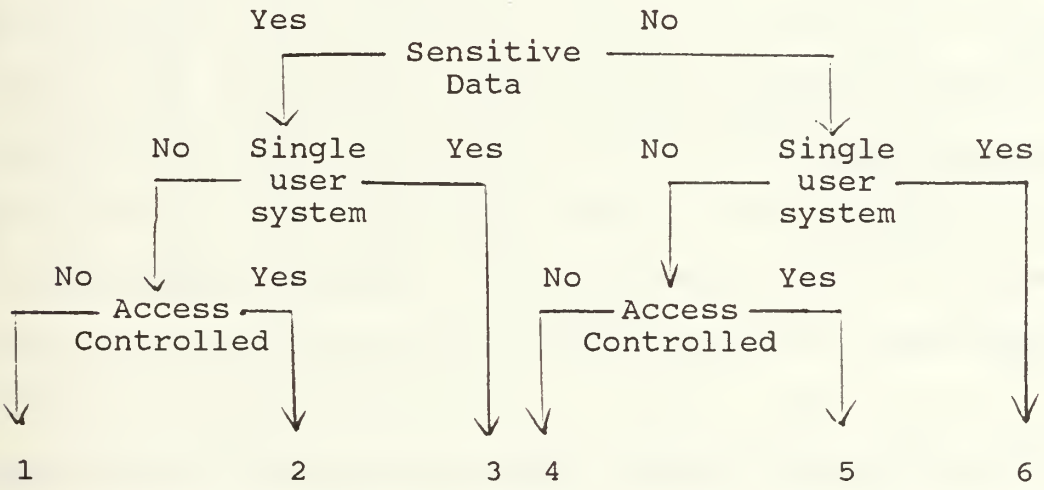


Figure 5.1. USGS Security Category Decision Tree

The category indicated by the tree diagram in Figure 5.1 is then found in the security requirements matrix (Table 5.1).

The letters in each column indicate by category whether the control or safeguard is required, suggested, or optional.

TABLE 5.1

SECURITY REQUIREMENTS MATRIX

Category	1	2	3	4	5	6
Risk analysis	R	R	R	R	R	R
Security officer	R	R	R	R	R	R
Continuity of operations	R	R	R	R	R	R
Procurement requirement	R	R	R	R	R	R
Physical security plan	R	R	R	R	R	S
ADP I, II, III	R	R	R	R	R	S
Training	R	R	R	R	R	S
Software certification	R	R	R	S	S	S
Separate libraries	R	R	O	S	S	O
Technical controls	R	R	O	O	O	O

R = required, S = suggested, O = optional

A typical USGA minicomputer site usually has at least one sensitive data base (Cecula, 1985). It would be used by a select group of people from the same office, placing it in category 3. The USGS baseline security model then mandates the following:

- conduct a risk analysis
- assign an information security officer
- review all positions requiring access to the computer system for security sensitivity and place each one into one of three position-sensitive categories
- develop a training program
- develop a physical security plan
- develop a continuity of operations program
- certify sensitive application software
- install reasonable physical safeguards
- future contracts must provide the appropriate security level.

C. ANALYSIS OF THE USGS BASELINE SECURITY MODEL

The positive aspect of the USGS model is that a determination as to which of the six categories is appropriate can be readily accomplished, thereby establishing categories of risk based upon system characteristics. This provides the conceptual basis for security baselines.

The negative aspect of this model is that all security categories require a risk analysis. Cecula states that risk analysis is time-consuming, costly, and often yields questionable results. Common sense dictates that these limitations are further exacerbated when the process is conducted by a person unskilled in information security.

The experience of agencies within the U.S. Geological Survey which use microcomputers extensively is that these agencies typically lack ADP expertise, particularly

individuals skilled in information security (Cecula, 1985). These factors seem to be reasonable expectations within the surface forces of the DON as well. This is because in all but the most unique circumstances, the requisite expertise will be unavailable aboard ships. It is not likely that individuals with the requisite skills will be billeted in ships, since the risk analysis process is mainframe/computer center oriented.

VI. A PROPOSED SOLUTION, THE NELSON/DOD MODEL

A. GENERAL

This model is based on the argument that the conventional risk analysis methodology is unsatisfactory. As discussed previously, the major problem with conducting risk analyses is the way that the ALE is calculated. The ALE has two components, the impact value rating (the impact, in dollars, of disclosure of sensitive data) and the threat values (the probability that the threat will occur). The ALE is the product of the impact value rating and the threat value, summed for each asset to yield the TOTAL ALE BY INDIVIDUAL THREAT. The ALEs for each individual threat are then summed to determine the TOTAL ALE (OPNAVINST 5239.1A, Sect. E.5.3). This procedure is the same as the expected value approach which is used for decision making under risk (Turban and Meredith, 1985). In the expected value approach, decision situations in which the chance (or probability) of occurrence of each state of nature is known (or can be estimated) are defined as decisions made under risk. The expected value of an alternative is the sum of all possible payoffs of that alternative, weighted by the probabilities of those payoffs occurring. Expected values calculated using subjective payoffs and probabilities (when payoffs and the probability that a particular state of

nature will occur must be estimated) are subject to the biases of the individuals making the estimations (Turban and Meredith, 1985).

The expected value $E(a_i)$ is defined as:

$$E(a_i) = p_1 o_{i1} + p_2 o_{i2} + \ldots = \Sigma_j p_j o_{ij}$$

where,

a_i = Alternative i

s_j = State of nature j

p_j = Probability that state of nature s_j will occur

o_{ij} = Payoff resulting from the selection of alternative a_i when s_j occurs

This method is based upon establishing a ceiling amount which should not be exceeded for providing safeguards and does not, therefore, lend itself to the identification of the most cost effective countermeasures. The expected value represents the maximum dollar amount that one should be willing to pay to safeguard the ADP system's assets. When dealing with Level I data, regardless of the ADP system configuration, the expected value approach using subjective probabilities may yield very large numbers. Level II data may also yield large values, but their characteristics are such that they are less likely to do so than Level I data.

Using the ROI of different countermeasures to prioritize their implementation can be misleading due to the limitations expressed above and in Chapter II (e.g., problems

associated with the complexity of accurately estimating asset values, estimating the probability that a particular state of nature will occur, and using these estimated values in expected value calculations). Again, expected value figures are only useful for determining the maximum dollar amount that one should be willing to pay to safeguard a system's assets. The reality of funding projects with limited budgets necessitates that cost effectiveness become a major consideration in system development.

B. PURPOSE

The purpose of this model is to provide a logical design, applicable in all ADP environments, which will identify the most cost effective means of providing for a particular system's security requirements. The focus of this model is on:

- designing a logical method which will identify minimum requirements based on system characteristics as defined by the ADP environment,
- identifying countermeasures which have been evaluated effective to meet the minimum requirement, and
- selecting countermeasures which have the lowest possible life cycle cost.

C. PROCEDURES

The remainder of this chapter is devoted to a discussion of the steps in the Nelson/DOD model which is intended to replace the risk analyses process used in the DON model. This model can be completed by the ADPSO with guidance from

the DAA. Using the Nelson/DOD model diagram (Appendix E) in conjunction with the following discussion is recommended.

1. Define the ADP Environment

a. Describe the system and its purpose, including manual systems being automated,

b. What is the system configuration;

- Hardware--mainframe, mini, micro, network, distributed system;
- Operating system--does the system require concurrent processing?
- What level of granularity[1] must the system support?
- Software--what applications programs will be used and what concurrency/data integrity problems may result?

c. What is the security mode of operation?

d. What level of information will be processed?

2. Is the ADP System Critical to the Activity's Mission

If the answer to 2. is No: Complete steps 3 through 7 and proceed to page 55, step 10.

If the answer to 2. is Yes: Continue to step 3.

3. Is the Security Environment Open or Closed

a. Closed Security Environment

The security environment is closed if both of the following conditions hold true.

a. Application developers (including maintainers, those individuals who maintain application programs) have

---

[1]In the concurrent processing environment, granularity refers to the level or degree to which resources will be reserved for a single process based on the particular scheduling algorithm being used. The levels of granularity may be specified at either the file, record, or field level.

sufficient clearances and authorizations to provide an acceptable presumption by those responsible for safeguarding classified data that the developers/maintainers have not introduced malicious logic. Sufficient clearance is defined as follows: where the maximum classification of data to be processed is Confidential or below, developers are cleared and authorized to the same level as the most sensitive data; where the maximum classification of data to be processed is Secret or above, developers have at least a Secret clearance.

b. Configuration control provides sufficient assurance that applications are protected against the introduction of malicious logic prior to and during operation of system applications (CSC-STD-001-83, Sect. 4.1.3.2.3).

b. Open Security Environment

The security environment is open if one of the following conditions holds true.

a. Application developers (including maintainers) do not have sufficient clearance or authorization to provide an acceptable presumption that they have not introduced malicious logic.

b. Configuration control does not provide sufficient assurance that applications are protected against the introduction of malicious logic prior to and during the operation of system applications.

- If Level I or II data is being processed and the system if operating in the open security environment, ensure that measures are taken which will place the system in the closed security environment.

4. What Unique Security Requirements Result from Using the ADP System?

Given the fact that Level I or II data are being processed, define threats which result from using the ADP system.

5. For Each Unique Security Requirement, Determine If Technical Controls/Countermeasures Are Necessary to Satisfy the Requirement

- If no: Use existing instructions pertinent to personal and information security/administrative and procedural controls (OPNAVINST 5510.1G).

- If Yes: 1) Calculate the risk index;

  2) Using the appropriate Table select the minimum criteria class (see Appendix F).

6. Do Products Exist Which Satisfy the Requirement

Check the Evaluated Products List for products which will satisfy the unique security requirement (see Appendix G). List all products which satisfy the requirement.

- If no "off-the-shelf" product exists, contract out (requirement = specification).

The purpose of this step is to identify a range of products with various performance characteristics and prices which will satisfy the particular security requirement and provide alternatives for the DAA. Since the cost of hardware and communications is decreasing, one alternative which the DAA should consider is purchasing additional hardware to be used in the dedicated mode for Level I and II applications.

7. Select the Most Cost Effective Countermeasure for Each Unique Requirement

The importance of the last two steps is to provide alternatives and introduce competition, the Federal Government's chosen method for controlling costs (OMB Circular No. A-109). Both provide a formalized framework which will

assist the DAA in introducing cost effectiveness into the decision process.

8. Calculate the Expected Value of the ADP system assets

The Expected Value of the ADP system assets provide a maximum cost to be spent on the ADP system.

9. Does the Expected Value Exceed the ADP System Cost Including Countermeasures and Implementation Costs

- If Yes, proceed with Step 2 of the Accreditation Process;
- If no, automating the system in the proposed configuration is not justifiable.

The purpose of this step is to determine if the Expected Value of the system exceeds the cost of the proposed ADP system including implemented countermeasures. If this is false then the cost of the system as configured is not justifiable.

10. Is Funding Available and Is the DAA Willing to Obligate Funds

- If no, continue using the manual system;
- If yes, continue to step 11.

11. Calculate the Expected Value of the ADP System Assets

The Expected Value of the ADP system assets provides a maximum cost to be spent on the ADP system.

12. Does the Expected Value Exceed the ADP System Cost Including Countermeasures and Implementation Costs?

- If yes, proceed with Step 2 of the Accreditation Process;
- If no, automating the system as configured is not justifiable.

D. ANALYSIS

The difference between the model proposed here and the OPNAV model is that the latter assumes the ADP system will be operating in the mainframe environment, while the former is more generally applicable.

Providing cost effective system security may require creativity. Unfortunately, at least intuitively, it seems that creativity is a function of the knowledge level of system designers. However, complex environments imply that systems designers are knowledgeable, so in this environment the problem is minimized. Less complex system configurations may, to a greater extent, employ administrative procedures, which will rely less on technical knowledge. Again, this minimizes the impact of the unavailability of technical expertise.

The model proposed here may replace the risk assessment process with a potentially more cost effective means of providing ADP system security. The model can be inserted into step (1) of the accreditation process listed below.

DON ACCREDITATION PROCEDURES, OPNAVINST 5239.1a:

(1) Use the Nelson/DOD Model to determine security requirements/countermeasures;

(2) Develop an ST&E Plan and conduct an ST&E;

(3) Document the ST&E test results;

a. if test results are unsatisfactory, iterate steps 1 and 2,

b. reevaluate in light of additional countermeasures proposed in previous iterations;

(4) Develop a Contingency Plan;

(5) Develop an AADPSP and submit it for COMNAVDAC approval;

(6) Prepare the accreditation support documentation;

(7) Issue a Statement of Accreditation;

(8) Forward information copies of the Statement of Accreditation to COMNAVDAC.

All countermeasures selected in step (7) define the Trusted Computing Base[2] (TCB).

---

[2]The Trusted Computing Base (TCB) is the totality of protection mechanisms within a computer system--including hardware firmware, and software--the combination of which is responsible for enforcing a security policy. It creates a basic protection environment and provides additional user services required for a trusted computer system. The ability of a trusted computing base to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user's clearance) related to the security policy.

VII. CONCLUSIONS AND RECOMMENDATIONS

A. SUMMARY

The intent of this thesis has been to evaluate the process whereby DON computer systems achieve accreditation. Emphasis has been placed on the accreditation process as it applies to shipboard microcomputer systems, which highlights some limitations inherent to OPNAVINST 5239.1A.

B. CONCLUSIONS

A basic conclusion of this thesis is that the DON has selected metrics which are inappropriate to the optimum selection of countermeasures. Risk analysis, the first step in the accreditation process, provides the means for identifying the threat and selecting countermeasures. Individual countermeasures are selected based on their respective ROI, the ratio of annual savings to the annual cost of additional countermeasures. The annual savings are calculated by subtracting the revised ALE from the original ALE. Two elements make up the ALE, the asset impact value and the threat values which are estimated for both the original and revised ALE's. These estimates are suspect because it can be argued that the values which comprise the ALE can be manipulated to justify expenditures for countermeasures. The argument made here is that given an ADP system is critical to an organization's mission,

countermeasures should be selected which systemically provide security in the most cost effective manner. The model developed in Chapter V is an attempt to accomplish this.

The issue of what countermeasures should be employed to secure shipboard microcomputer systems and achieve accreditation is also dealt with in Chapter V., The Nelson/DOD model proposes the use of administrative procedures and TEMPEST certification as the means to achieving shipboard microcomputer accreditation.

C. RECOMMENDATIONS

The analysis provided leads one to the conclusion that at least in this situation administrative structure lags well behind technical change. Within the DON, this problem transcends the usual difficulties experienced in updating documentation. Administrative lag is also manifested when directives are promulgated in that these directives typically have limited applicability and a short useful life.

Because OPNAVINST 5239.1A is mainframe/computer center oriented in an environment in which diverse mini- and microcomputer systems are becoming prevalent, it is such an instruction. There is, however, a remedy which provides some relief from this problem.

Nolan's Information System Life Cycle Model (Gibson and Nolan, 1974) demonstrates the evolutionary nature of an

organization's information systems (IS). While the model is not generally useful as a planning device, it can be used to determine an organization's position in the IS life cycle continuum. Once this position has been established, management has an indication of where the organization's ADP/MIS function is headed, given the organization's requirements. This information can then be used to generalized guidance and instructions in such a manner as to extend their applicability and overall usefulness.

Based on OPNAVINST 5239.1A and other factors, the author's conclusion is that the DON is in the contagion stage of Nolan's model. This stage is characterized by the unplanned (in the macro sense) proliferation of hardware and applications software with little emphasis being placed on information as an organization resource.

Organizations in the contagion stage are likely to experience problems associated with the proliferation of hardware and applications, while having few qualified individuals to perform necessary administrative functions. Management focus is on managing equipment rather than data. The problems experienced by the US Geological Survey and the DON associated with the lack of experienced personnel to provide analysis necessary for providing IS security is indicative of this situation.

The solution to the problems of too few qualified personnel and the necessity to conduct the complex computer

accreditation process is exacerbated by the size of the DON. In the short term, the solution to the accreditation problem depends upon the DON's ability to implement alternate means of determining an ADP system's countermeasures which rely less on formal risk analysis, such as the Nelson/DOD model.

However, the necessary conceptual elements comprising a possible long term solution are available. These elements are decision support systems (DSS) and distributed processing. DSS are characterized as interactive computer-based systems that help decision makers utilize data and models to solve unstructured problems (Sprague and Carlson, 1982). Distributed processing is defined as a system in which peripheral small processors can completely process a transaction but are subordinate to one or more central processors. The peripheral machines are linked to the center, and the entire complex is designed in a coordinated fashion. Programs and data bases are centrally prepared and down-line loaded into the peripheral machines (Martin, 1981).

A DSS could be developed which would assist in the process of determining an information system's most cost effective set of security countermeasures, leading to systems accreditation. In essence, Appendix E could be automated. The DSS could then be distributed, utilizing the Defense Data Network (DDN), to various locations such as

NARDACs, where local organizations could use the system with the assistance of NARDAC personnel.

The development of such a DSS requires the completion of the following, possibly as future research endeavors:

- creation of a dialog subsystem; the capabilities of the system must be articulated and implemented through the dialog;
- creation of a model subsystem; the capability to integrate data access and decision models (in this case the capability to model computer systems must be developed);
- creation of a data base subsystem; this entails automating the Evaluated Products List for Trusted Computer Systems, and
- link all components of the DSS using the DDN.

Unfortunately, this recommendation exceeds the DON's present data administration capabilities and should only be undertaken when the DON's IS have become much more mature. Ironically, at that point the DON's need for the DSS will be much less dramatic.

APPENDIX A

ADP SECURITY SURVEY

SECTION I. Basic Data.

1. System Identification: Shipboard Microcomputer System

   ( ) Office Information System

   (X) ADP System

   ( ) Network

2. System Description:

   In general, the system described here is intended to be representative of the type system presently being used in the shipboard environment, one which supports line functions aboard cruiser/destroyer type ships at sea. The system hardware components consist of a central processing unit, keyboard, CRT, and printer. System software consists of an operating system, word processing, and database programs. The personnel using the system are primarily officers and chief petty officers, but could include any individual owning a microcomputer who is using it aboard ship. System data includes classified and unclassified message drafts, information covered under the Privacy Act, and information specific to each department including custody items, personnel qualifications, inventories, etc. System procedures should, at a minimum, address

access controls, means to ensure data integrity, and backup and recovery.

3. Equipment Location: CO, XO, and Department Head's staterooms.

4. System Operations Contact for Security:

   Name: ADP Security Officer Code: _____

   Bldg: _____ Room: _____ Phone: _____

5. Type of Data Processed and Security Mode of Operation

TYPE OF DATA	PERCENT OF PROCESSING TIME	SECURITY MODE OF OPERATION*
Level I		
TOP SECRET	1	Dedicated Mode
SECRET	2	"
CONFIDENTIAL	8	"
Level II		
Privacy Act	19	"
For Official Use Only	10	"
Financial	10	"
Sensitive Management	10	"
Level III	40	"
TOTAL	100%	

(*Note: Applicable security modes are: Compartmented, Controlled, Dedicated, System High, Multilevel, Limited Access, as defined in Appendix A of OPNAVINST 5239.1A.)

6. Operating System and Standard Application Software Identifications:

   Any IBM PC Compatible DOS operating system, word processing, database management system, etc.

7. Scope of System: (Check all that apply.)

   (X) Stand-alone and single controlled area (single CPU with single workstation).

( ) Shared logic and single controlled area (single CPU with multiple workstations).

( ) Shared logic and more than one controlled area (single CPU with multiple workstations).

( ) Multiple processors and single controlled area (multiple CPUs)

( ) Used with a remote computer _____ percent of the time.

(X) Other: Multiple stand-alone microcomputers and multiple controlled areas (many CPUs with many workstations).

8. Total Value of System: $6,000 (Dollar value impact of loss and cost to replace).

A. Equipment: $5,000

B. Software: $1,000

C. Data: $0

The Level I data used in this system is transitive in nature. The predominant use of this data is in classified message drafts. Because it is not a stored data base the associated security problem is greatly reduced.

The $0 value for data is justified if 3 conditions are met:

- the system achieves TEMPEST certification,
- training is conducted to maximize operator proficiency, thereby reducing operator error, unintentional disclosure of Level I data, and data entry errors, and
- management procedures mandate periodic back-up of all software data files.

9. Mission Relatedness

A. Primary Function(s) of the System or network:

The function of the shipboard microcomputer system is to provide a more convenient means of conducting administration. This is accomplished by providing

the CO, XO, and Department Heads a more expeditious means of accessing, updating, and manipulating data. The system also facilitates the preparation of messages.

B. Contingency Plan Requirement:

Because the system is not mission critical, a contingency plan is not required. A loss of processing capability for a reasonable period of time would not adversely affect the ship's mission. If alternate hardware exists, its location shall be specified as well as the location of data/software diskettes, back-up diskettes, and supplies.

Section II. Site Security Profile and Minimum Requirements for Environmental and Physical Security.

1. Vulnerability: Temperature or Humidity Outside Normal Range.

Operating Countermeasures: (Check all that apply.)

(x) Adequate heating and controls
(x) Adequate cooling and controls
( ) Only designated personnel operate controls
( ) Functioning temperature and humidity recorder
( ) Functioning temperature/humidity warning system
( ) Other: _____

Assessment of Risk:

( ) High ( ) Moderate (x) Low

2. Vulnerability: Inadequate Lighting or Electrical Service.

Operating Countermeasures: (Check all that apply.)

(X) Adequate primary lighting
(X) Adequate emergency lighting

(X) Adequate periodic checks of emergency lighting
(X) Adequate primary power and outlets
( ) Functioning power filters or voltage regulators
(X) Available backup power
( ) Other: Battery back-up for soft fail capability

Assessment of Risk:

( ) High (X) Moderate ( ) Low

3. Vulnerability: Improper Housekeeping.

Operating Countermeasures: (Check all that apply.)

(X) Routine cleaning schedule is adhered to
( ) Cleaning personnel are trained in computer room procedures
( ) An ADP facility representative is present during cleaning
( ) Dust contributors are not permitted in equipment area (outer coats, throw rugs, drapes, venetian blinds, etc.)
(X) Air-conditioning filters are cleaned/replaced regularly
(X) Floors are polished with non-flake wax using proper buffer materials or properly damp-mopped
( ) Carpet areas are vacuumed frequently and anti-static spray is used regularly
( ) Smoking, eating, and drinking are not permitted in equipment areas
( ) Other: _____

Assessment of Risk:

( ) High ( ) Moderate (X) Low

4. Threat: Water Damage.

Operating Countermeasures: (Check all that apply.)

(X) Water/steam pipes are not located above equipment
(X) Water/steam pipes are inspected at regular intervals
( ) Functioning humidity warning system
( ) Dry pipe sprinkler system
( ) Plastic sheets available to cover susceptible equipment

(X) Water detection devices
( ) Other: _____

Assessment of Risk:

( ) high ( ) Moderate (X) Low

5. Threat: Fire.

Operating Countermeasures: (Check all that apply.)

(X) Up-to-date fire bill posted
(X) Periodic fire drills
(X) Training--fire prevention methods
(X) Training--emergency power down procedures
(X) Training--knowledge of fire detection system
(X) Training--use of fire extinguishers
(X) Training--use of fire alarm system
( ) Training--evacuation plan
(X) Training--individual responsibilities in case of fire
( ) Functioning emergency power-off switches
(X) Sprinkler system installed
( ) Halon system installed
(X) Carbon dioxide fire extinguisher installed
( ) Smoke/heat detectors installed
(X) Functioning fire alarm system
( ) Emergency exits clearly marked
( ) Other: _____

Assessment of Risk:

( ) High ( ) Moderate (X) Low

----------				In existence
|	----------			Being developed
|	|	-------		Required but no action taken
|	|	|	--	Not required
( )	(X)	( )	( )	Security Operating Procedures Handbook
( )	( )	( )	( )	Line diagrams showing interconnection of components and physical layout
( )	(X)	( )	( )	Description of countermeasures in place
( )	( )	( )	( )	Copies of previous accreditation or interim authority to operate
( )	(X)	( )	( )	TEMPEST accreditation request
( )	( )	( )	( )	TEMPEST accreditation test results
( )	( )	( )	( )	Physical accreditation (for SCI data only)
( )	(X)	( )	( )	ST&E Test Plan
( )	( )	( )	( )	Contingency Plan
( )	( )	( )	( )	Contingency Plan test results

( ) (X) ( ) ( ) Formal Risk Assessment
( ) ( ) ( ) ( ) Other (specify): _____

SECTION IV. Survey Data.

1. Current Status:

( ) Operating under accreditation for processing Level _____ data in _____ security mode of operation. Accreditation granted by _____. Dated _____. (Attach a copy of statement of accreditation.)

( ) Operating under interim authority for processing Level _____ data in _____ security mode of operation. Interim authority granted by _____. Dated _____. Expires _____. (Attach a copy of interim authority to operate.)

2. Survey Prepared By:

Name: _____ Code: _____
Bldg: _____ Room: _____ Phone: _____

To the best of my knowledge, the information provided in this survey and the attached documentation is complete and accurate.

Signature _____ Date _____

6. Vulnerability: Unauthorized Physical Access.

Operating Countermeasures: (Check all that apply.)

(X) Perimeter fence (access to quarterdeck controlled)
(X) Security guards (petty officer of the watch armed)
(X) Building secured outside of normal working hours
( ) Area alarms (motion detectors, open door detectors, perimeter penetration detectors)
(X) Authorized access list
( ) Cypher door lock
( ) Combination door lock
(X) Recognition of authorized personnel
( ) Closed circuit television
( ) Administrative procedures
( ) Physical isolation/protection
( ) High employee morale

( ) Close supervision of employees
(X) Indoctrination of personnel in security awareness
( ) Other: _____

Assessment of Risk:

( ) High ( ) Moderate ( ) Low

SECTION III. Current status of accreditation support documentation. (Applies to all ADP activities and networks which will be authorized to handle Level I or Level II data.)

1. All ADP activities and networks which will be authorized to handle Level I or II data must either be accredited or be granted interim authority to operate pending accreditation. Accreditation is based on supporting documentation including a risk assessment. This section provides a statement of the current status of the accreditation support documentation. (Check all that apply.)

APPENDIX B

RISK ASSESSMENT, METHOD II

Completing the Risk Assessment Matrix and the Additional Countermeasures Selection Worksheet satisfies the requirements for Method II. Risk Assessment Matrix #1 is provided to illustrate how easily large sums of money can be justified. In this case $377,025 is the TOTAL ALE.

However, TEMPEST certification eliminates the Eavesdropping threat and a training program encompassing system use and administrative procedures will substantially reduce the unintentional operator error, unintentional disclosure, and unintentional data entry error threats.

Only those countermeasures not already a part of the system are included in the calculations. Risk Assessment Matrix #2 indicates the threats which have not yet been countered and the Additional Countermeasures Selection Worksheet indicates the appropriate countermeasures.

RISK ASSESSMENT MATRIX #1

THREAT	ASSETS AND THEIR IMPACT VALUE (a) Micro System $5,000	(b) Software $1,000	(c) TS Data $1,000,000	(d) S Data $100,000	(e) C Data $10,000	(f) FOUO Data $1,000	(g) $	TOTAL ALE BY INDIVIDUAL THREAT
1 Eavesdropping	TV 0 0	TV 0	TV H 330K	TV H 33K	TV H 3300	TV H 330	TV	366,630
2 Unintentional Output Error	0 0	0	L 3K	L 300	L 30	L 3		3,333
3 Unintentional Disclosure	0 0	.0	L 3K	L 300	L 30	L 3		3,333
4 Unintentional Data Entry Error	0 0	0	L 3K	L 300	L 30	L 3		3,333
5 Power Instability	M 165	M 33	0 0	0 0	0 0	0 0		198
6 Water Damage	M 165	M 33	0 0	0 0	0 0	0 0		198
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
21								
22								
23								
24								
TOTAL ALE BY INDIVIDUAL ASSET	330	66	339K	33,900	3,396	339		TOTAL ALE 377,025

OPNAV 5239/12 (2-82) * TV (THREAT VALUE) L (LOW) M (MEDIUM) H (HIGH)

RISK ASSESSMENT MATRIX #2

THREAT	ASSETS AND THEIR IMPACT VALUE (a) Micro system $5,000	(b) Software $1,000	(c) TS Data $1,000,000	(d) S Data $100,000	(e) C Data $10,000	(f) FOUO Data $1,000	(g) $	TOTAL ALE BY INDIVIDUAL THREAT
1 Power Instability	TV M 165	TV M 33	TV O O	TV O O	TV O O	TV O O	TV	198
2 Water Damage	TV M 165	TV M 33	TV O O	TV O O	TV O O	TV O O	TV	198
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
21								
22								
23								
24								
TOTAL ALE BY INDIVIDUAL ASSET	330	66	0	0	0	0		TOTAL ALE 396

OPNAV 5239/12 (2-82) • TV (THREAT VALUE) L (LOW) M (MEDIUM) H (HIGH)

ADDITIONAL COUNTERMEASURES SELECTION WORKSHEET

A ADDITIONAL COUNTERMEASURES	B THREATS PAIRED	C ORIGINAL ALE	D REVISED ALE	E ANNUAL SAVINGS	F ANNUAL COST OF ADDITIONAL COUNTERMEASURES	G RETURN ON INVESTMENT	H ADDITIONAL COUNTERMEASURES PRIORITIES
1 Surge Protector	Power Instability	198	18	180			
	ANNUAL SAVINGS SUBTOTAL			180	80	2.25:1	2
2 Plastic Covers	Water Damage	198	18	180			
	ANNUAL SAVINGS SUBTOTAL			180	32	5.63:1	1
3							
	ANNUAL SAVINGS SUBTOTAL						
4							
	ANNUAL SAVINGS SUBTOTAL						
5							
	ANNUAL SAVINGS SUBTOTAL						

APPENDIX C

DEVELOPMENT, CONDUCT AND REPORTING OF SECURITY TEST AND EVALUATIONS

1. PURPOSE.

1.1. For ST&Es that are preceded by Method I risk assessments, the checklist (Appendix C) will be used to aid in the identification of countermeasurers and vulnerabilities required for completion of Appendix A.

1.2. For ST&Es that are preceded by a Method II risk assessment, the checklist will be used to obtain the data required for the DAAs to assure the system is operating within an acceptable level of risk.

2. ORGANIZATION.

2.1. The checklist is divided into 2 sections: Section I contains general activity-wide questions; Section II contains system-specific questions.

2.2. Each question has three possible answers: yes, no, and not applicable (N/A). 'Yes' means the requirements addressed in the question have affirmatively been met. 'No' means that some level of risk exists. 'N/A' means that the subject matter addressed does not apply to the system being evaluated. A line of comments has been provided after each question for further explanations as required.

3. PROCEDURES.

3.1. For ST&Es preceded by Method I risk assessments, complete the checklist and use the results in conjunction with the risk assessment to aid in the identification of vulnerabilities and countermeasures in Appendix A.

3.2. For ST&Es prceded by Method II risk assessments, complete the checklist and use the results to develop an ST&E report for submission to the DAA. Ensure the report addressess all questions answered with a "NO."

SECTION I

ACTIVITY

		YES	NO	N/A
1.	Has an ADP Security Program been established?	___	___	___
	Comments: _____			
2.	Has an Activity ADP Security Plan (AADPSP) been developed?	___	___	___
	Comments: _____			
3.	Has the AADPSP been approved by the Naval Data Automation Command (NAVDAC) Code 51?	___	___	___
	Comments: _____			
4.	Has the Designated Approving Authority granted activity accreditation?	___	___	___
	Comments: _____			
5.	Is the AADPSP updated as changes occur?	___	___	___
	Comments: _____			
6.	Is there evidence that top-level management supports the ADP Security program through such requirements as security awareness training, documented security procedures, etc.?	___	___	___
	Comments: _____			
7.	Is the ADP security staff sufficient to support the ADP Security Program?	___	___	___
	Comments: _____			

	YES	NO	N/A
8. Has an ADP Security Officer (ADPSO) been appointed in writing by the Commanding Officer?	___	___	___

Comments: _____

_____

9. Does the ADPSO have a strong technical background and experience in the administration of ADP systems?	___	___	___

Comments: _____

_____

10. Has the ADPSO received training on OPNAVINST 5239.1A?	___	___	___

Comments: _____

_____

11. Have the duties and responsibilities of the ADPSO been defined in writing?	___	___	___

Comments: _____

_____

12. Do the duties and responsibilities of the ADPSO include:

a. Coordinating with the command security manager on matters concerning ADP security, in accordance with the security organizational structure established by the Commanding Officer?	___	___	___

Comments: _____

_____

b. Developing and maintaining an ADP Security Plan (ADPSP)?	___	___	___

Comments: _____

_____

c. Ensuring that a Network Security Officer (NSO) is appointed for networks which are sponsored by the activity?	___	___	___

Comments: _____

_____

	YES	NO	N/A
d. Ensuring that ADP System Security Officers (ADPSSOs) are appointed in writing where applicable?	___	___	___

Comments: _____

_____

e. Ensuring that Terminal Area Security Officers (TASOs) are appointed where applicable for each remote facility? ___ ___ ___

Comments: _____

_____

f. Ensuring that an effective activity Risk Management Program is implemented? ___ ___ ___

Comments: _____

_____

g. Ensuring that all ADP security incidents or violations are investigated, documented and reported to appropriate authorities? ___ ___ ___

Comments: _____

_____

h. Ensuring that security requirements are included in life cycle management documentation as prescribed in SECNAV Instructions 5000.1A or 5231.1A as appropriate? ___ ___ ___

Comments: _____

_____

i. Ensuring that all procurement documents or specifications approved within the activity comply with ADP security requirements? ___ ___ ___

Comments: _____

_____

j. Ensuring the contracts (DD Form 254) include statement(s) ensuring contractor compliance with Navy ADP Security requirements? ___ ___ ___

Comments: _____

_____

	YES	NO	N/A
k. Ensuring the development and testing of all contingency plans?	___	___	___

Comments:_____

_____

l. Ensuring the NAVAUDSVC is advised of the development of an ADP system, as applicable?	___	___	___

Comments:_____

_____

m. Ensuring that accreditation documentation is developed and maintained?	___	___	___

Comments:_____

_____

n. Assisting the ADP security staff in implementing their respective ADP security requirements?	___	___	___

Comments:_____

_____

o. Ensuring that applicable personnel security procedures are established?	___	___	___

Comments:_____

_____

p. Ensuring that Security Test and Evaluations (ST&Es) are conducted where applicable?	___	___	___

13. If this activity sponsors a network:

a. Has a Network Security Officer (NSO) been appointed in writing?	___	___	___

Comments:_____

_____

b. Have the duties and responsibilities of the NSO been defined in writing?	___	___	___

Comments:_____

_____

	YES	NO	N/A
c. Do the duties and responsibilities of the NSO include:			
(1) Ensuring that countermeasures and security requirements are in the network design and that individual nodes of the network comply with these countermeasures and requirements, prior to interfacing with the network?	___	___	___

Comments: _____

_____

(2) Ensuring that security measures and procedures used at network nodes fully support the security integrity of the network?	___	___	___

Comments: _____

_____

(3) Maintaining liaison with all ADPSSOs in the network?	___	___	___

Comments: _____

_____

(4) Ensuring that all required countermeasuers are utilized?	___	___	___

Comments: _____

_____

14. Are all ADP security violation/incidents reported to the ADPSO?	___	___	___

Comments: _____

_____

15. Do newly assigned ADP personnel receive briefings on:

a. ADP security procedures of the activity	___	___	___

Comments: _____

_____

b. Marking, handling and accountability of classified ADP information?	___	___	___

Comments: _____

_____

	YES	NO	N/A
c. Marking, handling and accountability of ADP sensitive, unclassified information?	___	___	___

Comments:_____

_____

d. ADP emergency procedures?	___	___	___

Comments:_____

_____

SECTION II

SYSTEM

A. NAME OF SYSTEM: _____

B. TYPE OF SYSTEM

	YES	NO	N/A
1. Office Information System (OIS)			
a. Has an Office Information System Security Officer (OISSO) been appointed in writing?	___	___	___
Comments: _____			
b. Have the duties and responsibilities of the OISSO been defined in writing by the ADPSO?	___	___	___
Comments: _____			
c. Do the duties and responsibilities of the OISSO include:	___	___	___
Comments: _____			
(1) Being the focal point of all security matters for the OIS systems assigned?	___	___	___
Comments: _____			
(2) Executing the ADP Security Program as it applies to the assigned OIS systems including preparing and supporting the accreditation support documentation?	___	___	___
Comments: _____			
(3) Maintaining an inventory of all OIS hardware, system software and major functional appplication systems?	___	___	___
Comments: _____			

	YES	NO	N/A
(4) Monitoring system activity (e.g., identification of the levels and types of data handled by the OIS systems, assignment of passwords, review of audit trails, etc.) to ensure compliance with security directives and procedures?	___	___	___

Comments: _____

(5) Maintaining liaison with remote facilities served by the OIS systems to ensure compliance with applicable security requirements?	___	___	___

Comments: _____

(6) Conducting and documenting risk assessments for the assigned OIS systems?	___	___	___

Comments: _____

(7) Supervising, testing and monitoring, as appropriate, changes in the OIS system affecting the ADP activity posture?	___	___	___

Comments: _____

(8) Implementing appropriate counter-measures required by directive or determined cost effective?	___	___	___

Comments: _____

(9) Assisting the ADPSO in implementing a comprehensive Activity ADP Security Program?	___	___	___

Comments: _____

(10) Developing and testing annual contingency plans for the assigned OIS systems?	___	___	___

Comments: _____

	YES	NO	N/A
(11) Monitoring OIS procurements for security impact to ensure compliance with security regulations and known security requirements for the assigned OIS systems?	___	___	___

Comments: _____

d. If the OIS system has remote terminals:

(1) Have TASOs been appointed?	___	___	___

Comments: _____

(2) Have the duties and responsibilities of the TASOs been defined in writing?	___	___	___

Comments: _____

(3) Do the duties and responsibilities of the TASO include:

(a) Serving as a single point of contact at his terminal area for the OISSO?	___	___	___

Comments: _____

(b) Implementing and enforcing all security requirements established by the OISSO for remote terminal areas?	___	___	___

Comments: _____

(c) Ensuring all countermeasures for remote terminal areas are in place?	___	___	___

Comments: _____

(d) Developing terminal security procedures for OISSO approval?	___	___	___

Comments: _____

	YES	NO	N/A
(e) Maintaining a current access list of remote devices?	___	___	___

Comments: _____

(f) Reporting security abnormalities to the OISSO or his designated representative?	___	___	___

Comments: _____

(g) Returning to the OISSO products that cannot be identified or which contain extraneous data?	___	___	___

Comments: _____

(4) Have security requirements been agreed to in writing between the host site and remote device sites?	___	___	___

Comments: _____

2. ADP System

a. Has an ADP System Security Officer (ADPSSO) been appointed in writing?	___	___	___

Comments: _____

b. Have the duties and responsibilities of the ADPSSO been defined in writing?	___	___	___

Comments: _____

c. Do the duties and responsibilities of the ADPSSO include:

(1) Being the focal point for all security matters for the ADP systems assigned?	___	___	___

Comments: _____

		YES	NO	N/A
(2)	Executing the ADP Security Program as it applies to the assigned ADP systems including preparing and supporting the accreditation support documentation?	___	___	___

Comments: _____

(3)	Maintaining an inventory of all hardware, system software and major functional application systems?	___	___	___

Comments: _____

(4)	Monitoring system activity (e.g., identification of the levels and types of data handled by the ADP systems, assignment of passwords, review of audit trails, etc.) to ensure compliance with security directives and procedures?	___	___	___

Comments: _____

(5)	Maintaining liaison with remote facilities served by the ADP systems to ensure compliance with applicable security requirements?	___	___	___

Comments: _____

(6)	Maintaining liaison with remote facilities served by the ADP system to ensure that a terminal area security officer (TASO) is designated by the served activity where applicable?	___	___	___

Comments: _____

(7)	Conducting and documenting risk assessments for the assigned ADP systems?	___	___	___

Comments: _____

	YES	NO	N/A
(8) Supervising, testing and monitoring, as appropriate, changes in the ADP system affecting the ADP activity posture?	___	___	___

Comments: _____

(9) Implementing appropriate countermeasures required by directive or determined cost effective?	___	___	___

Comments: _____

(10) Assisting the ADPSO in implementing a comprehensive Activity ADP Security Program?	___	___	___

Comments: _____

(11) Developing and testing annual contingency plans for the assigned ADP systems?	___	___	___

Comments: _____

(12) Monitoring ADP procurements for security impact to ensure compliance with security regulations and known security requirements for the assigned ADP systems?	___	___	___

Comments: _____

d. If the ADP system is a node of a network:

(1) Have security requirements been agreed to in writing by the network DAA and the ADP facility DAA of the network?	___	___	___

Comments: _____

(2) Has an ADPSO been appointed in writing for the node?	___	___	___

Comments: _____

	YES	NO	N/A
e. If the ADP system has remote terminals:			
(1) Have Terminal Area Security Officers (TASOs) been appointed?	___	___	___

Comments: _____

(2) Have the duties and responsibilities of the TASOs been defined in writing?	___	___	___

Comments: _____

(3) Do the duties and responsibilities of the TASO include:			
(a) Serving as a single point of contact at his terminal area for the ADPSSO?	___	___	___

Comments: _____

(b) Implementing and enforcing all security requirements established by the ADPSSO for remote terminal areas?	___	___	___

Comments: _____

(c) Ensuring all countermeasures for remote terminal areas are in-place?	___	___	___

Comments: _____

(d) Developing terminal security procedures for ADPSSO approval?	___	___	___

Comments: _____

(e) Maintaining a current access list of remote devices?	___	___	___

Comments: _____

(f) Reporting security abnormalities to the ADPSSO or his designated representive?	___	___	___

Comments: _____

	YES	NO	N/A
(g) Returning to the ADPSSO ADP products that cannot be identified or which contain extraneous data?	___	___	___

Comments: _____

(4) Have security requirements been agreed to in writing between the host site and remote device sites?	___	___	___

Comments: _____

C. SYSTEM ACCREDITATION

	YES	NO	N/A
1. Is this system accounted for on the ADPSO's inventory?	___	___	___

Comments: _____

2. Has a survey (Figure E-1 in OPNAVINST 5239.1A) been completed on this system?	___	___	___

Comments: _____

3. Have security operating procedures been developed for this system?	___	___	___

Comments: _____

4. Has the DAA determined if a risk assessment is required?	___	___	___

Comments: _____

5. If a risk assessment is required:

a. Has the risk assessment been performed?	___	___	___

Comments: _____

b. Do the ADPSO and ADPSSO maintain a copy of the risk assessment?	___	___	___

Comments: _____

c. Is the risk assessment kept updated and repeated:

(1) At least every 5 years?	___	___	___

Comments: _____

(2) When any change is made to the facility, ADP equipment, system software or application software which effects the overall ADP security posture?	___	___	___

Comments: _____

	YES	NO	N/A
(3) When any change is made in operational configuration, data sensitivity, or classification level?	___	___	___

Comments: _____

(4) When any change is made which appears to invalidate the original conditions of accreditation?	___	___	___

Comments: _____

6. Has a Security Test and Evaluation (ST&E) been prepared (only for systems processing Level I or II data) which is sufficiently comprehensive to ensure thorough examination and exercising of the system's security control features and procedures and/or in combination, to determine their effectiveness and reliability?	___	___	___

Comments: _____

7. Has an ST&E been performed to determine the effectiveness of countermeasures employed in maintaining the security of the system at an acceptable level of risk?	___	___	___

Comments: _____

8. Do the ADPSO and ADPSSO maintain a copy of the ST&E plan and results?	___	___	___

Comments: _____

9. Is a contingency plan for this system in existence?	___	___	___

Comments: _____

10. Does the contingency plan, at a minimum, address:

a. The actions required to minimize the impact of a fire, flood, civil disorder, natural disaster, or bomb threat?	___	___	___

Comments: _____

	YES	NO	N/A
b. Backup procedures to conduct essential ADP operational tasks after a disruption to the primary ADP facility?	___	___	___

Comments: _____

c. Recovery procedures to permit rapid restoration of the ADP facility following physical destruction, major damage or loss of data?	___	___	___

Comments: _____

11. Does the contingency operations plan provide for:

a. Local storage of tapes and punched cards in the central computer facility in metal or other fire retardant cabinets?	___	___	___

Comments: _____

b. Duplicate system tapes, startup decks, data base save tapes, and site-unique application program card files or tapes to be maintained in a secure location removed from the central computer facility?	___	___	___

Comments: _____

c. Identification of an alternate site containing compatible equipment?	___	___	___

Comments: _____

d. Destruction or safeguarding of classified material in the central computer facility in the event that the facility must be evacuated?	___	___	___

Comments: _____

12. Has the contingency plan been tested during the past year?	___	___	___

Comments: _____

13. Do the ADPSO and ADPSSO maintain a copy of the Contingency Plan?	___	___	___

Comments: _____

	YES	NO	N/A
14. Do the ADPSO and ADPSSO maintain a copy of the Contingency Plan Test and Evaluation Report?	___	___	___

Comments: _____

	YES	NO	N/A

D. HUMAN RESOURCES SECURITY

1. Do all personnel having unescorted access to the system possess a clearance and a need-to-know equal to or higher than the highest classification and all categories of data being processed? ___ ___ ___

Comments: _____

2. Is an access roster maintained at each entry point to the central computer facility and remote terminal area? ___ ___ ___

Comments: _____

3. Are escort procedures established for controlling visitors to the central computer facility and remote terminal areas? ___ ___ ___

Comments: _____

a. Are all potential escorts properly briefed on their responsibilities? ___ ___ ___

Comments: _____

b. Is a record of all visitors maintained for 12 months? ___ ___ ___

Comments: _____

4. During operational hours is the central computer facility manned by at least two cleared personnel? ___ ___ ___

Comments: _____

5. Are all unescorted maintenance personnel cleared for the highest level and all restrictive categories of classified information in the system? ___ ___ ___

Comments: _____

	YES	NO	N/A
6. Are escorts provided for maintenance personnel who are not appropriately cleared?	___	___	___

Comments: _____

7. Are escorts technically competent to review the maintenance work performed?	___	___	___

Comments: _____

8. Are procedures to delete and add personnel to access lists implemented, including the notification of all concerned ADP security officials?	___	___	___

Comments: _____

	YES	NO	N/A

E. PHYSICAL SECURITY

1. Does the computer facility meet the following requirements?

a. Is the system operated within the manufacturer's optimum temperature and humidity range specifications? ___ ___ ___

Comments: _____

b. Are environmental systems dedicated to the computer facility? ___ ___ ___

Comments: _____

c. Are environmental controls regulated by key designated personnel only? ___ ___ ___

Comments: _____

d. Is a temperature/humidity recording instrument installed to monitor the system area? ___ ___ ___

Comments: _____

(1) Is the temperature/humidity instrument connected to an alarm to warn of near-limit conditions? ___ ___ ___

Comments: _____

e. Is there adequate lighting? ___ ___ ___

Comments: _____

f. Is there emergency lighting? ___ ___ ___

Comments: _____

g. Are periodic checks made of the emergency lighting? ___ ___ ___

Comments: _____

	YES	NO	N/A
h. Is electrical power reliable?	___	___	___

Comments: _____

i. Are there voltage regulators or other electronic devices to prevent serious power fluctuations?	___	___	___

Comments: _____

j. Is there an uninterruptible power source for the facility?	___	___	___

Comments: _____

k. Are cleaning procedures and schedules established and adhered to?	___	___	___

Comments: _____

l. Is an ADP representative present during cleaning operations?	___	___	___

Comments: _____

m. Is the facility overhead free of steam and water pipes?	___	___	___

Comments: _____

n. Are plastic sheets available to protect the system from water damage?	___	___	___

Comments: _____

o. Is there a facility fire bill?	___	___	___

Comments: _____

p. Are emergency exits clearly marked?	___	___	___

Comments: _____

q. Do employees receive periodic training in the following areas:			
(1) Power shut down and start up procedures?	___	___	___

Comments: _____

	YES	NO	N/A
(2) Operation of emergency power?	___	___	___

Comments: _____

(3) Operation of fire detection and alarm system?	___	___	___

Comments: _____

(4) Operation of fire suppression equipment?	___	___	___

Comments: _____

(5) Building evacuation procedures?	___	___	___

Comments: _____

r. Is there a master power switch to all ADP equipment?	___	___	___

Comments: _____

s. Is the master power switch located near the main entrance of the ADP area?	___	___	___

Comments: _____

t. Is the master power switch adequately labeled to prevent accidental shut off?	___	___	___

Comments: _____

u. If the system processes critical applications, is there a sequential shut down routine?	___	___	___

Comments: _____

v. Is there a sufficient number of portable fire extinguishers?	___	___	___

Comments: _____

		YES	NO	N/A
w.	Is there a central fire suppression system?	___	___	___

Comments: _____

x.	Is there automatic smoke/fire detection equipment?	___	___	___

Comments: _____

y.	Does the smoke/fire detection equipment activate an alarm at the nearest fire station?	___	___	___

Comments: _____

z.	Are there warning signs posted outside tape vaults and other magnetic storage areas to warn fire fighters of toxic fumes?	___	___	___

Comments: _____

aa.	If the facility does not operate 24-hours, is there a guard force employed after hours and on weekends?	___	___	___

Comments: _____

bb.	Is the guard force briefed on emergency procedures?	___	___	___

Comments: _____

cc.	Is the guard force provided with an emergency recall bill?	___	___	___

Comments: _____

dd.	Are physical access controls implemented to prevent unauthorized entry into the computer facilities and remote terminal areas?			

Comments: _____

		YES	NO	N/A
ee.	Are visitor control procedures in place?	___	___	___

Comments: _____

ff.	Are positive personnel identification measures (e.g., badge system, fingerprints) in place?	___	___	___

Comments: _____

	YES	NO	N/A

F. COMMUNICATIONS SECURITY

1. Do all communications links between remote terminal areas and the central computer facility meet the requirements for the transmission of the highest classification and for all categories of data which are contained in the system? ___ ___ ___

Comments: _____

2. Are all remote terminals uniquely identified when accessing the host? ___ ___ ___

Comments: _____

3. Are all dial-up terminals disabled from connection to the central computer facility during classified processing periods? ___ ___ ___

Comments: _____

	YES	NO	N/A
G. EMANATIONS SECURITY			
1. If the ADP system processes Level I data:			
a. Has a TEMPEST vulnerability assessment been requested?	___	___	___
Comments: _____			
b. Has a TEMPEST vulnerability assessment been performed?	___	___	___
Comments: _____			
(1) Does it represent the current equipment configuration?	___	___	___
Comments: _____			
c. Are all changes, repairs, and modifications to TEMPEST certified ADPE controlled so that equipment emanation characteristics are not altered?	___	___	___
Comments: _____			

	YES	NO	N/A
H. HARDWARE SECURITY			
1. Is the site SOP manual used for configuring system hardware?	___	___	___
Comments:_____			
2. Are switch settings for each hardware unit specified for each system?	___	___	___
Comments:_____			
3. Are scheduled maintenance activities monitored to ensure proper reliability and performance?	___	___	___
Comments:_____			
4. Are periods of down time verified?	___	___	___
Comments:_____			

	YES	NO	N/A

I. SOFTWARE SECURITY

1. Is the authenticity of the operating system or executive software verified by comparing the registry or shipment number of the software package with that contained in record communications from the originator? ___ ___ ___

Comments: _____

2. Prior to operational use of any new system release, does the ADPSSO conduct sufficient testing to verify that the system meets the documented and approved security specifications? ___ ___ ___

Comments: _____

3. Are testing and debugging of new releases performed during dedicated time in a controlled environment? ___ ___ ___

Comments: _____

4. Are all site-unique patches tested by system software personnel? ___ ___ ___

Comments: _____

5. Is a log of all system patches maintained and monitored by the ADPSSO? ___ ___ ___

Comments: _____

6. Are all modifications to the operating system cross-checked by two appropriately cleared operating system programmers? ___ ___ ___

Comments: _____

7. Are startup procedures executed as described in the site SOP manual? ___ ___ ___

Comments: _____

	YES	NO	N/A
8. Are system tapes identified in a unique manner to distinguish them from non-system tapes?	___	___	___

Comments: _____

9. Are system tapes protected to the highest classification and for all restrictive categories of data which the central system is processing or storing online?	___	___	___

Comments: _____

10. Has a method to control access to system tapes or disks been developed and approved by the ADPSSO?	___	___	___

Comments: _____

11. Is the ADPSSO informed of all unauthorized requests for system tape access?	___	___	___

Comments: _____

12. Are system module source listings made available to site personnel only on a need-to-know basis and are the listings physically protected as FOUO?	___	___	___

Comments: _____

13. Has each individual user been assigned a unique user identification and password which has been randomly, machine generated?	___	___	___

Comments: _____

14. Is a password changed:

a. Whenever an individual knowing a log-on password is transferred, discharged, reassigned or the individual's security clearance is reduced, suspended, or removed by proper authority?	___	___	___

Comments: _____

	YES	NO	N/A
b. Whenever a password or record of password has been compromised, or is suspected of being compromised?	___	___	___

Comments: _____

c. At least annually?	___	___	___

Comments: _____

15. Is removable media controlled at the highest level of data processed and restricted to users cleared for that level?	___	___	___

Comments: _____

16. When no longer needed, are data purged or declassified?	___	___	___

Comments: _____

17. Does an audit record identify the reason for system shutdown or crash?	___	___	___

Comments: _____

18. Are system dumps taken following a system crash?	___	___	___

Comments: _____

19. Are system dumps reviewed by the ADPSSO or site analyst?	___	___	___

Comments: _____

20. Is all memory purged between periods processing?	___	___	___

Comments: _____

21. Are security specifications coordinated by site management prior to approval of application software development and maintenance?	___	___	___

Comments: _____

	YES	NO	N/A
22. Are application software design reviews conducted, documented, and maintained as official records of the site?	___	___	___

Comments:_____

23. Are system tests of new application releases conducted?	___	___	___

Comments:_____

24. If operational user files are required for testing, are only copies of the files used?	___	___	___

Comments:_____

	YES	NO	N/A

J. ADMINISTRATIVE SECURITY

1. Are effective procedures for limiting access to the system and its data established and implemented? ___ ___ ___

Comments: _____

2. Does the ADPSSO maintain a current roster of all personnel authorized access to the system? ___ ___ ___

Comments: _____

3. Does the ADPSSO control the distribution of passwords? ___ ___ ___

Comments: _____

4. Are log-on passwords for unclassified systems marked For Official Use Only (FOUO)? ___ ___ ___

Comments: _____

5. Are working papers containing classified information marked with:

   a. Date of creation? ___ ___ ___

Comments: _____

   b. Highest classification of any information contained in the product? ___ ___ ___

Comments: _____

6. Are printed listings containing classified information marked with the security classification on the top and bottom of each page? ___ ___ ___

Comments: _____

7. Are microfilm and microfiche conspicuously marked on the microform media or its container with the overall security classification so as to be readable with unaided eye? ___ ___ ___

Comments: _____

	YES	NO	N/A
8. Are all ADP storage devices externally marked with:			
a. The overall security classification?	___	___	___
Comments: _____			
b. Special access restrictions?	___	___	___
Comments: _____			
c. A permanently assigned identification/control number?	___	___	___
Comments: _____			
9. Do magnetic tapes have a gummed label affixed containing:			
a. Tape classification/declassification?	___	___	___
Comments: _____			
b. Tape identification control number?	___	___	___
Comments: _____			
10. Are removable disk packs marked with the same information required for magnetic tapes?	___	___	___
Comments: _____			
11. Are customers responsible for reviewing and verifying the actual classification of the product?	___	___	___
Comments: _____			
12. Are effective procedures for protecting personal and other unclassified sensitive data established and implemented?	___	___	___
Comments: _____			
13. Have procedures for maintaining an inventory of all removable magnetic storage devices been established?	___	___	___
Comments: _____			

	YES	NO	N/A
14. Is the inventory listing for devices classified TOP SECRET or special category verified at least semiannually?	___	___	___

Comments: _____

15. Is the inventory listing for devices classified SECRET and below verified at least annually?	___	___	___

Comments: _____

16. Is magnetic storage media being declassified and disposed of as required by Appendix C of OPNAVINST 5239.1A?	___	___	___

Comments: _____

17. Are security incidents investigated to determine their cause, and where possible, the corrective action to be taken?	___	___	___

Comments: _____

18. Are ADP security incidents fully documented and properly reported?	___	___	___

Comments: _____

APPENDIX D

CONTINGENCY DATA FORM

System Identification _____

Code/Location _____

ADPSSO _____

Key User _____

Alternate System Location _____

Service Contract Identification _____

Location of Data/Software Diskettes _____

Location of Diskette Backups _____

Location of Supplies (i.e, ribbons, printwheels, etc.) _____

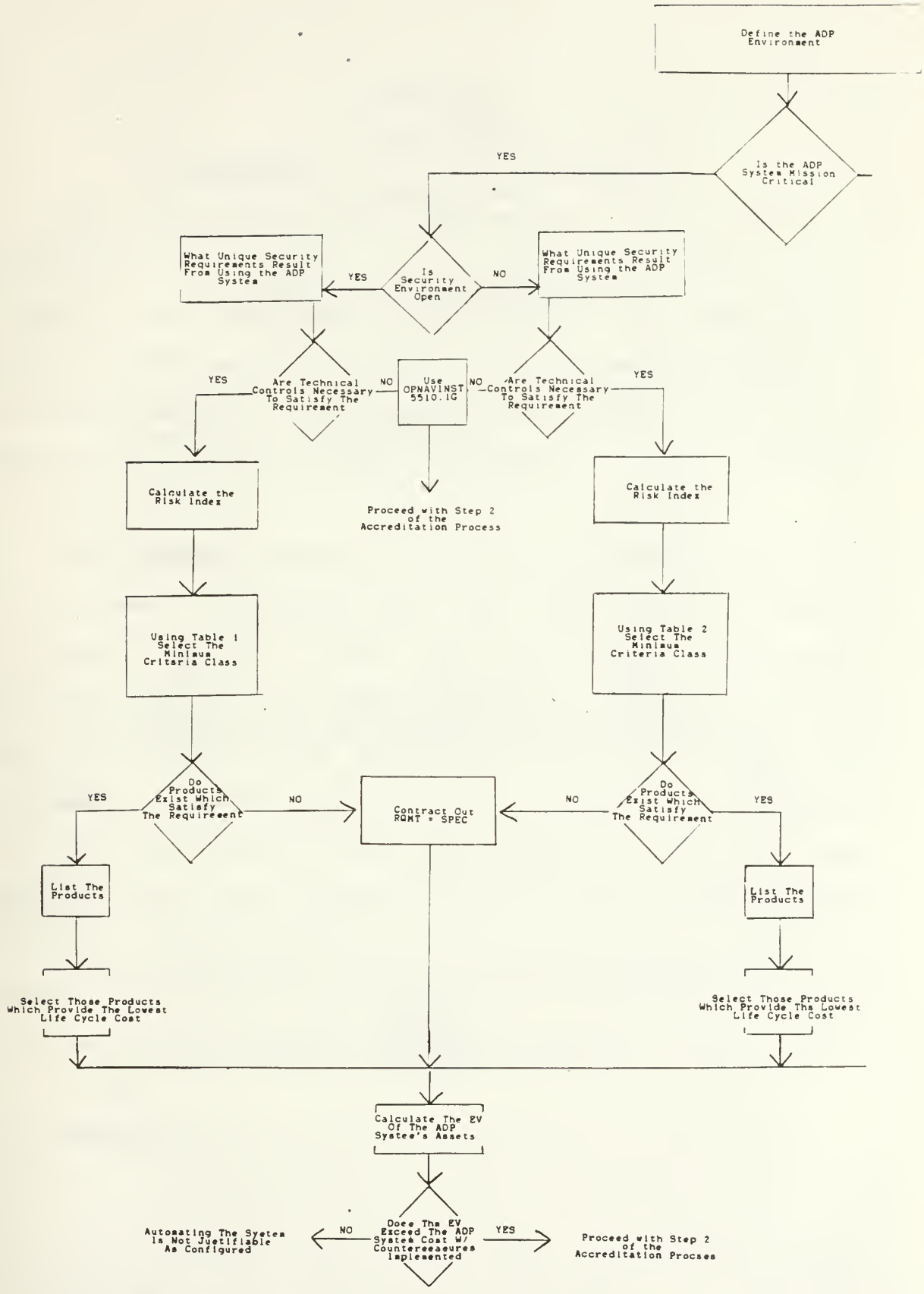
List of Authorized Users

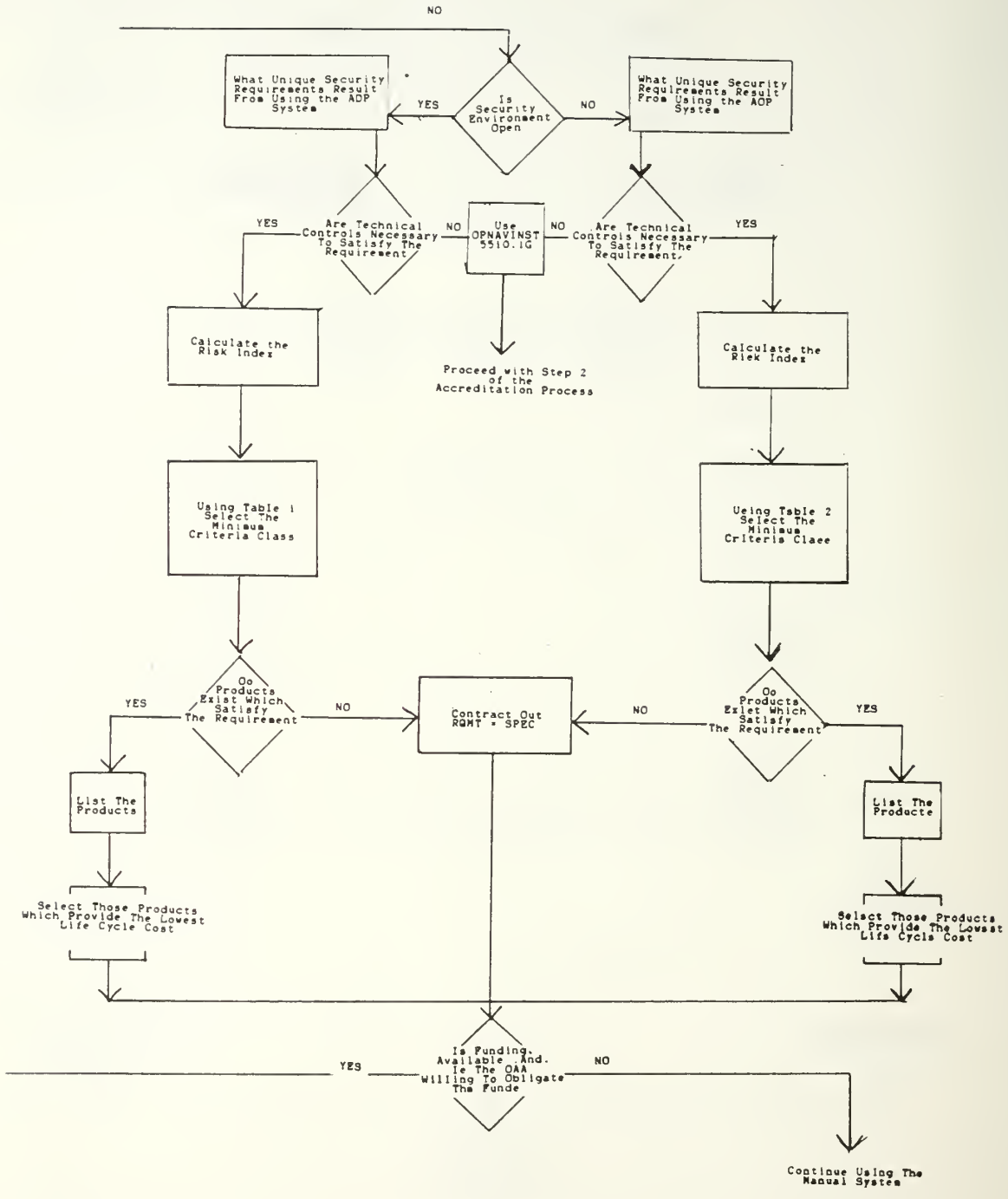
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

APPENDIX E

THE NELSON/DOD MODEL DIAGRAM

The Nelson/DOD model diagram is intended to be used in conjunction with Chapter VI.


Define the ADP Environment
Is the ADP System Mission Critical
YES
Is Security Environment Open
YES
NO
What Unique Security Requirements Result From Using the ADP System
What Unique Security Requirements Result From Using the ADP System
Are Technical Controls Necessary To Satisfy The Requirement
YES
NO
Use OPNAVINST 5510.1G
Are Technical Controls Necessary To Satisfy The Requirement
NO
YES
Calculate the Risk Index
Proceed with Step 2 of the Accreditation Process
Calculate the Risk Index
Using Table 1 Select The Minimum Critsria Class
Using Table 2 Select The Minimum Criteria Class
Do Products Exist Which Satisfy The Requirement
YES
NO
Contract Out RQMT = SPEC
NO
Do Products Exist Which Satisfy The Requirement
YES
List The Products
List The Products
Select Those Products Which Provide The Lowest Life Cycle Cost
Select Those Products Which Provide The Lowest Life Cycle Cost
Calculate The EV Of The ADP Systee's Assets
Doee The EV Exceed The ADP Systee Cost W/ Countereeaeures Implemented
NO
YES
Automating The Systee Is Not Juetifiable As Configured
Proceed with Step 2 of the Accreditation Procses


NO
What Unique Security Requirements Result From Using the ADP System
YES
Is Security Environment Open
NO
What Unique Security Requirements Result From Using the ADP System
YES
Are Technical Controls Necessary To Satisfy The Requirement
NO
Use OPNAVINST 5510.1G
NO
Are Technical Controls Necessary To Satisfy The Requirement
YES
Calculate the Risk Index
Proceed with Step 2 of the Accreditation Process
Calculate the Risk Index
Using Table 1 Select The Minimum Criteria Class
Using Table 2 Select The Minimum Criteria Class
Do Products Exist Which Satisfy The Requirement
YES
NO
Contract Out RQMT + SPEC
NO
Do Products Exist Which Satisfy The Requirement
YES
List The Products
Select Those Products Which Provide The Lowest Life Cycle Cost
List The Products
Select Those Products Which Provide The Lowest Life Cycle Cost
Is Funding Available And Is The OAA Willing To Obligate The Funds
YES
NO
Continue Using The Manual System

APPENDIX F

RISK INDEX

The evaluation class appropriate for a system is dependent on the level of security risk inherent to that system. This risk is referred to as that system's risk index. Risk index is defined as the disparity between the maximum clearance of the least cleared system users and the maximum sensitivity of data processed by a system (CSC-STD-003-85).

The Computer Security Requirements are based upon this risk index. Although there are other factors that can influence security risk, such as mission criticality, required denial of service protection, and threat severity, only the risk index is used to determine the minimum class of trusted computer system[1] to be employed, since it can be uniformly applied in the determination of security risk. The risk index for a system depends on the rating associated with the system's minimum user clearance (R_{min}) taken from Table 1 and the rating associated with the system's maximum data sensitivity (R_{max}) taken from Table 2.

---

[1]A system that employs sufficient hardware and software integrity measures to allow its use for processing simultaneously a range of sensitive or classified information.

The risk index is computed as follows:

Case a. If R_{min} is less than R_{max}, then the risk index is determined by subtracting R_{min} from R_{max}.[2]

$$\text{Risk Index} = R_{max} - R_{min}$$

Case b. If R_{min} is greater than or equal to R_{max}, then:

Risk Index = 1, if there are categories on the system to which some users are not authorized access;

= 0, otherwise (i.e., if there are no categories on the system or if all users are authorized access to all categories).

---

[2]There is one anomalous case in which this formula gives an incorrect result. This is the case where the maximum data sensitivity is Top Secret/Background Investigation and the maximum data sensitivity is Top Secret. According to the formula, this gives a risk index of 1. In actuality, the risk index in this case is zero. The anomaly results because there are two "levels" of Top Secret clearance and only one level of Top Secret data.

TABLE 1

COMPUTER SECURITY REQUIREMENTS FOR OPEN SECURITY ENVIRONMENTS

RISK INDEX	SECURITY OPERATING MODE	MINIMUM CRITERIA CLASS[1]
0	Dedicated	No Prescribed Minimum[2]
0	System High	C2[3]
1	Limited Access, Controlled, Compartmented, Multilevel	B1[4]
2	Limited Access, Controlled, Compartmented, Multilevel	B2
3	Controlled, Multilevel	B3
4	Multilevel	A1
5	Multilevel	*
6	Multilevel	*
7	Multilevel	*

[1]The asterisk (*) indicates that computer protection for environments with that risk index are considered to be beyond the state of current technology. Such environments must augment technical protection with personnel or administrative security safeguards.

[2]Although there is no prescribed minimum, the integrity and denial of service requirements of many systems warrant at least class C1 protection.

[3]If the system processes sensitive or classified data, at least a class C2 system is required. If the system does not process sensitive or classified data, a class C1 system is sufficient.

[4]Where a system processes classified or compartmented data and some users do not have at least a Confidential clearance, or when there are more than two types of compartmented information being processed, at least a class B2 system is required.

TABLE 2

COMPUTER SECURITY REQUIREMENTS FOR CLOSED SECURITY ENVIRONMENTS

RISK INDEX	SECURITY OPERATING MODE	MINIMUM CRITERIA CLASS[1]
0	Dedicated	No Prescribed Minimum[2]
0	System High	C2[3]
1	Limited Access, Controlled, Compartmented, Multilevel	B1[4]
2	Limited Access, Controlled, Compartmented, Multilevel	B2
3	Controlled, Multilevel	B2
4	Multilevel	B3
5	Multilevel	A1
6	Multilevel	*
7	Multilevel	*

[1]The asterisk (*) indicates that computer protection for environments with that risk index are considered to be beyond the state of current technology. Such environments must augment technical protection with physical, personnel, and/or administrative safeguards.

[2]Although there is no prescribed minimum, the integrity and denial of service requirements of many systems warrant at least class C1 protection.

[3]If the system processes sensitive or classified data, at least a class C2 system is required. If the system does not process sensitive or classified data, a class C1 system is sufficient.

[4]Where a system processes classified or compartmented data and some users do not have at least a Confidential clearance, at least a class B2 system is required.

APPENDIX G

THE EVALUATED PRODUCTS LISTS FOR TRUSTED COMPUTER SYSTEMS

The Department of Defense Computer Security Center (DoDCSC) was established in January 1981. The primary goal of the DoDCSC is to encourage the widespread availability of trusted computer systems, systems that employ sufficient hardware and software integrity measures to be used for simultaneously processing a range of sensitive or classified information (CSC-STD-001-83).

The primary means by which this goal is achieved is through the DoDCSC's Commercial Product Evaluation Program. This program is focused on the technical evaluation of the protection capabilities of off-the-shelf commercially produced and supported systems that meet the computer security needs of government departments and agencies. Product evaluation results are published in an Evaluated Products List (EPL) which is independent of any consideration of overall system performance, potential applications or particular processing environment. The EPL provides an authoritative evaluation of a system's relative suitability for use in processing sensitive information.

The DoD Trusted Computer System Evaluation Criteria is the standard against which products are evaluated. The "Criteria" are divided into four divisions: D (minimal protection), C (discretionary protection), B (mandatory

protection), and A (verified protection), ordered in a hierarchal manner with the highest division (A) being reserved for systems providing the most comprehensive security.

Each division represents a major improvement in the overall confidence one can place in the system for the protection of sensitive information. These divisions are based on features and assurances to support three types of security requirements: policy, accountability and assurance.

Generally speaking, secure systems use specific security features to control access to information such that only properly authorized individuals, or processes operating in their behalf, will have read or write access capabilities. Six fundamental requirements are necessary to support this objective:

Policy

Requirement 1--SECURITY POLICY--there must be an explicit and well-defined security policy enforced by the system.

Requirement 2--MARKING--Access control labels must be associated with objects.[1]

---

[1]An object is a passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples of objects are: records, blocks, pages, segments, files, directories, directory trees, and programs.

Accountability

Requirement 3--IDENTIFICATION--Individual subjects must be identified.

Requirement 4--ACCOUNTABILITY--Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party.

Assurance

Requirement 5--ASSURANCE--The computer system must contain hardware/software mechanisms that can be independently evaluated to provide sufficient assurance that the system enforces requirements 1 through 4 above.

Requirement 6--CONTINUOUS PROTECTION--The trusted mechanisms that enforce these basic requirements must be continuously protected against tampering and/or unauthorized changes.

The products on the EPL have been evaluated against the Criteria and assigned an Overall Evaluation Class rating. The security evaluation of a product is contained in a formal report (NTIS). The Overall Evaluation Class (product rating) in the EPL is the highest class for which the evidence for the product demonstrates that all the requirements in the Criteria have been met.

LIST OF REFERENCES

Cash, James I., Jr., McFarlan, F. Warren, and McKenney, James L., Corporate Information Systems Management: Test and Cases, 1st Ed., p. 29, Richard D. Irwin, Inc., 1983.

Cecula, Adolph F., Jr., "Consider Alternatives to Formal Risk Analysis," Government Computer News, September 27, 1985.

Department of Defense, CSC-STD-001-83, Department of Defense Trusted Computer System Evaluation Criteria, p. 48, August 15, 1983.

Department of Defense, CSC-STD-003-85, Computer Security Requirements, p. 7, June 25, 1985.

DEVOKE Data Products, pp. 34, 67, Devoke, Summer/Fall 1985.

Martin, James, Design and Strategy for Distributed Data Processing, 1st Ed., p. 90, Prentice-Hall, Inc., 1981.

Nolan, Richard L., Managing the Data Resource Function, 2nd Ed., West Publishing Co., St. Paul, Minnesota, 1982.

OMB Circular No. A-109, Office of Management and Budget, p. 7, April 5, 1976.

Perry, William E., "Micro Security Is No Different: People Are Its Focus," Government Computer News, May 9, 1986.

Sharp, Laurie, NARDAC, San Francisco, telephone conversation with author, June 1986.

Sprague, Ralph H., Jr. and Carlson, Eric D., Building Effective Decision Support Systems, 1st Ed., p. 4, Prentice-Hall, Inc., 1982.

Turban, Efraim and Meredith, Jack R., Fundamentals of Management Science, 3rd Ed., p. 66, Business Publications, Inc., 1985.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6145	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, California 93943-5002	2
3.	Ken J. Euske, Code 54Ee Department of Administrative Sciences Naval Postgraduate School Monterey, California 93943-5000	1
4.	Daniel R. Dolk, Code 54Dk Department of Administrative Sciences Naval Postgraduate School Monterey, California 93943-5000	1
5.	Computer Technology Programs, Code 37 Naval Postgraduate School Monterey, California 93943-5000	1
6.	Bruce E. Nelson, LT USN Department Head School Class 96 Surface Warfare Officers School Command Newport, Rhode Island 02841	1
7.	Commanding Officer Navy Regional Data Automation Center, San Francisco Naval Air Station Alameda, California 94501 Attn: Laurie Sharp	1

220333

Thesis
N3584
c.1

Nelson
Shipboard microcomputers and the ADP accreditation process.